ISSN 2278-5612

Privacy Factors of Social Network That Effect Users Trust And Confidentiality

Nader Yahya Mohamed Alkeinay[1], Norita Md Norwawi[2], Fauziah Abdul Wahid[3], Roesnita Ismail[4], Najwa Hayaati Mohd Alwi[5]

[1,2,3,4,5]Universiti Sains Islam Malaysia (USIM) – Faculty if science and technology - Bandar Baru Nilai, 71800 Nilai, Negeri Sembilan, Malaysia

Abstract

Social network is term used to refer to the social structure that is made up of a set of social actors. The social actors in this case include organizations or individuals. Social networks allow people to interact and socialize as they get to learn and know each other. Through social networking sites, people from different parts of a country or the world also get to meet and interact. However, there have been issues with regards to social network privacy for those who use the internet to use social network sites. This paper will look at some of the factors that affect trust of the users as well as the privacy issues related to social networks (Fernandez, 2009).

Keywords: Social network; Privacy model; factors effecting trust

Council for Innovative Research

Peer Review Research Publishing System

Journal: International Journal of Management & Information Technology

Vol. 8, No. 3
editor@cirworld.com
www.cirworld.com, member.cirworld.com

Introduction

A good number of organizations tend to search the internet, particularly social networking sites as one of the ways of background checks. By doing so, they can come across incriminating or embarrassing posts from the past that may prevent an individual from getting hired or getting a given position. Similar checks are also conducted by other institutions including universities. Given that such institutions may ask one to join or like their pages before the application process, privacy options may not help much. Privacy is one of the highest concerns for social network users. Protecting personal information as well as the sensitive information of others as people continue going online to use social sites such as Facebook, tweeter and linked in among others(Susan, 2006). There are a number of potential dangers that include;

Personal attacks

Through harvesting of personal information by cyber criminals, such data or information may be used against a user. Such information may also be used for a variety of other attacks including physical stalking and tampering with online settings of a given user.

Harming employers

Sensitive information has been used by criminal and competitors against employers. Such information may include those posted by employees, and may also be used in damaging the reputation of an entire organization.

Users have encountered a range of problems with regard to social network. Some of the most common dangers associated with social networking include;

Data theft- data theft takes place when cyber criminals are able to hack in to the account of a given user. By doing so, they can learn and obtain a good amount of information about the user as well as that of the friends and family of the user. Data theft also helps these criminals to be able to steal the identity of the user (identity theft).

Viruses- viruses are majorly received once the user has been tricked in to visiting given site that contains potential harmful viruses. Once the user has visited the site, the virus may run automatically on the user's pc.

Masquerading- masquerading takes place when the user interacts with people pretending to be someone important, or some one the user knows. By doing so, the user may not feel at risk sharing personal information with the other party.

Social network security

On the social sites, information about individuals will typically spread faster as compared to the real- life network. This information may be used to damage the reputation of a person depending on the information shared and spread through the network. However, there are some networks such as Facebook that contain structures that allow the user settings that are meant to protect them. Through the settings, one can choose who to share information with, and who not to. However, they change from time to time, and a user may not have all the information and knowledge about them (Saint, 2010).

Different sites will vary in the degree of privacy provided. For instance, Facebook allows one to share a range of personal information such as current address, date of birth, names as well as their telephone numbers. Others also encourage people to share more personal information such as status, area of residence, hobbies and interests among others. On the other hand, other sites encourage people to be less open about this type of information, and therefore people tend to remain anonymous.

Concerns have been raised due to the fact that users are displaying significant amount of information on the social networks that may in the long last have serious implications on their privacy. Particularly, Facebook has faced criticism due to the perceived negligence with regard to default settings. This is because once an update is made by a user, the default settings occur, and therefore any changes that had been made are reversed (Fernandez, 2009).

A good number of security issues continue to be posed, and according to a study conducted on social media, 2000 respondents were asked whether they had seen spam, malware of phishing incidents. Of the respondents in the study, 71 percent reported that they personally, or a friend of theirs had been spammed on social media site. 46 percent of the respondents had been phished whereas 45 percent of them received malware (Xi and Michael, 2012).

Social engineering is one of the tools that has been used by cybercriminals to steal information about another user from a social network profile and posts. Attacks are then tailored on the interests and likes of the user. This is also another factor that has affected trust of the users and has made the threats to security rather difficult to recognize.

Factors affecting user's trust

With a social network site like Facebook, the user does not necessarily help in making money, but advertiser do. Given that the advertisers would love to share their messages to as many users as possible, Facebook typically shares information about a user to just about everyone apart from friends, which further raises concerns about security (Saint, 2010).

Some of the other tools that have been used to enhance scamming include;

Cross- site scripting

Through a number of messages such as `Facebook dislike button' a user is taken to a webpage that encourages the user to cut and past malicious java script code in to an address bar of a browser. However, attacks from self-xss (cross-site scripting) have the ability to run while hidden. This allows malware to be installed without the knowledge of a user.

Click jacking

Also referred to as UI redressing, this is a technique that prompts users to reveal personal information. However, the malicious technique can also take control of the user's pc once they click on an innocuous webpage. It takes the form of an embedded code or script, which can execute without the user knowing that it is happening.

Survey scams

This is also related to click jacking, and the user is prompted to install applications that are from a spammed link. Through new topics, the scammer is able to take advantage by taking the user to another fake sit such as YouTube, and tricked in to completing a survey. By taking the survey, the scam is virally spread to other Facebook friends.

Data storage

In a majority of the social network sites, users are required to agree to the `terms of use policy' during registration. Studies have shown that the terms will typically contain in them clauses that allow operators to store users information and data and even share such with a third party.

Moreover, some of the sites make it difficult to delete an account du to the fact that the site operators tend to hold on to the data and information about a user even after the deactivation of an account. These may result in the sharing with third parties information and data about a given user or users (Molva & Strufe, 2009).

There have also been number of other factors that have affected trust of the users including;

Identity theft

Given that users are encouraged to share a large volume of personal information, it has become easier to estimate social security numbers of users that can be used for identity theft. Many people have claimed of cases where their accounts have been hacked in to just to be used for damaging the reputation of a user.

Stalking

Stalking of users has become very common, which is as a result of the sharing of personal information. By sharing such information, an individual is able to locate a user. Some of the sites allow user to determine and locate a friend wherever they are, which has raised controversy. Aol is one of such sites that has faced criticism over such applications that enable a user to track anther user without their knowledge.

Minimizing the risks

To minimize the risks, the users of social networks have to be careful about who they share information with, and the amount of information they share online. Reducing the amount of posts on these sites is also another means of reducing risks of privacy. It is also critical that users use hard to guess passwords, not share their passwords with others and be more careful about sites they are not sure of in addition to links that may increase such risks (Rosenblum, 2007).

References

[1] Saint, n. 2010. Facebook's response to privacy concerns: "if you're not comfortable sharing, don't". [online]. Available at: http://www.businessinsider.com/facebooks-response-to-privacy-concerns-if-youre-not-comfortable-sharing-dont-2010-5

[2] Fernandez, p. 2009. Online social networking sites and privacy: revisiting ethical considerations for a new generation of technology. [online]. Available at: http://digitalcommons.unl.edu/cgi/viewcontent.cgi?article=1250&context=libphilprac

[3] Xi chen and katina michael. "privacy issues and solutions in social network sites" ieee technology and society magazine 31.4 (2012): 43-53.

[4] L. Cutillo, r. Molva & t. Strufe, "privacy preserving social networking through decentralization," in proc of 6th international conference on wireless ondemand network systems and services, feb 2009, pp. 145-152.

[5] D. Rosenblum, "what anyone can know: the privacy risks of social networking sites," ieee security and privacy, vol. 5 (3), pp. 40-49, 2007.

[6] Susan b. Barnes (september 4, 2006). A privacy paradox: social networking in united states, first monday, volume 11, number 9,