How safe are we? Security risks of the social networks

Maša Kojić, Serbia

Abstract

Nowadays, we are witnessing an extreme proliferation of the social networks. The proliferation of social networks can be seen in two ways: as an expansion of social network websites, but also as an increase in the number of people who are starting to use them. This phenomenon is accompanied by a number of risks that users are exposed to every time they create an account on some social network website or leave some information on it. The problem becomes more serious bearing in mind that most users are not aware of these risks. This situation favors those who are willing to abuse the information of other people.

Security risks of social networks can be different, but are mostly connected with the user's privacy. The term 'privacy' in this paper is used in its broadest sense, including not only the user's personal data, but also every other piece of data concerning the user's movement, activities, likes, plans…

The other question, which is very important concerning security risks of social networks, centres on responsibility for those risks. It could be concluded that both users and social network providers are responsible for the user's security on the networks. However, in order to hold somebody liable for users' security, this liability should be proscribed and presented to the users before they start to use social network websites. Today, we have privacy policy rules or some other rules, but not all security risks are covered by these. This paper seeks to answer whether the rules proscribed so that social network providers can distance themselves from possible abuses are really designed to help the users be safe?

Keywords: user safety; social network sites; social network providers; privacy; privacy policies

Introduction

'A social network is a social structure made up of individuals (or organizations) called "nodes", which are tied (connected) by one or more specific types of interdependency, such as friendship, kinship, common interest, financial exchange, dislike, sexual relationships, or relationships of beliefs, knowledge or prestige' (Wikipedia, 2011a).

Since their establishment, social networks have attracted the attention of a great number of people, exceeding the number of individuals involved in their establishment. Each type of social network was established by people not aiming to establish global 'project'. It seems to me as if it was unintentional.

Although, there are differences between different social networks, they have at least one characteristic in common. In order to use some of the social networks, it is necessary to create a user profile which includes giving personal and, sometimes, confidential information concerning the user's private or business life.

In recent years, individuals and institutions, both governmental and non-governmental, are raising awareness of the risks attached to the use of social networks. There are many people ready to misuse the information that people make available on the Internet. Social networks in particular contribute to that and therefore, it is very important to raise awareness of those risks and to find out how those risks could be reduced.

People often do not think about those risks, feeling that there are safe, but, actually, staying safe on social networks means being aware of all the risks involved and trying to avoid them.

This document has been produced by DiploFoundation with the financial assistance of the European Union. The contents of this document are the sole responsibility of the author and can under no circumstances be regarded as reflecting the position of the European Union or DiploFoundation.

The most popular Social Network websites

Examples of the most popular social network websites:

Facebook: a social networking website that allows people to communicate with their friends and exchange information.

MySpace: a social networking website offering an interactive, user-submitted network of friends, personal profiles, blogs and groups, commonly used for sharing photos, music and videos.

Ning: an online platform for creating social websites and social networks aimed at users who want to create networks around specific interests or have limited technical skills.

Twitter: a website which offers a social networking and microblogging service, enabling its users to send and read messages called tweets. Tweets are text-based posts of up to 140 characters displayed on the user's profile page. Tweets are publicly visible by default; however, senders can restrict message delivery to just their followers. Users may subscribe to other users' tweets – this is known as following and subscribers are known as followers.

Youtube: a video-sharing website on which users can upload, share, and view videos.

Flickr: an image-hosting and video-hosting website, web services suite, and online community created by Ludicorp and later acquired by Yahoo!.

A lot of security incidents have occurred on social networks since their establishment, partly because, first of all, there is a lack of knowledge and a lack of caution on the part of users, but, there are also security omissions by the social networks providers. With the increase of social network sites, the number of users, and the amount of information available through those networks, security risks are increasing. For instance, on one of the most popular social network sites, Facebook, people update their status to show where are they going next weekend, where their kids are, how much money they earn… not caring that somebody could misuse this information. 'Seven days in Paris with the family' might seem a totally harmless status, but actually, through this status you are saying that your house will be empty for seven days while you are in Paris. This is very useful information for burglars!

Furthermore, a lot of phishing attacks have occurred on social networks sites such as Facebook, MySpace and Twitter, where attackers have managed to alienate the profiles of a certain number of users. Using these profiles, the attackers sent phishing messages to everyone on the users' lists of friends. These messages contained a malicious link to illegal websites that looked the same as the original social networking site. Users who entered their user names and passwords were at risk, because attackers had control of the counterfeit site.

The security risks of social networks can be divided into four groups: (1) the threats to user's privacy, (2) the threats to the networks, (3) threats to the user's identity, and (4) threats to society.

The history of social networks

The history of social networks started with the BBS (Bulletin Board System). 'A Bulletin Board System, or BBS, is a computer system running software that allows users to connect and log in to the system using a terminal program. Once logged in, a user can perform functions such as uploading and downloading software and data, reading news and bulletins, and exchanging messages with other users, either through electronic mail or in public message boards' (Wikipedia, 2011b). This system was established in the late 1970s. BBSs gained popularity throughout the 1980s and well into the 1990s.

In 1997, SixDegrees.com was established. This was the first website that allowed its users to create profiles, invite friends, organise groups, and surf other user profiles. It was based on Hungarian, Frigyes Karinthy's theory, later popularised by a play written by John Guare, that everyone is on average approximately six steps away from any other person on Earth. In 2002, SixDegrees.com was succeeded by Friendster. This service 'allows users to contact other members, maintain those contacts, and share online content and media with those contacts. The website is also used for dating and discovering new events, bands, and hobbies. Users may share videos, photos, messages and comments

with other members via their profile and their network; (Wikipedia, 2011c). 'Friendster used a degree of separation concept similar to that of the now-defunct SixDegrees.com, refined it into a routine dubbed the "Circle of Friends" (wherein the pathways connecting two people are displayed), and promoted the idea that a rich online community can exist only between people who truly have common bonds. And it ensured there were plenty of ways to discover those bonds' (Nickson, 2009). Some people think that Friendster deserves special mention because it was the first popular website that contained all of the features we expect from social networks today — especially the notion of using a social graph to track relationships. The next two years were the most important when it comes to the popularity of the social networks. In 2003, MySpace was discovered and in 2004, Facebook.

Besides those mentioned, there were and still are, a lot of other social network websites. This

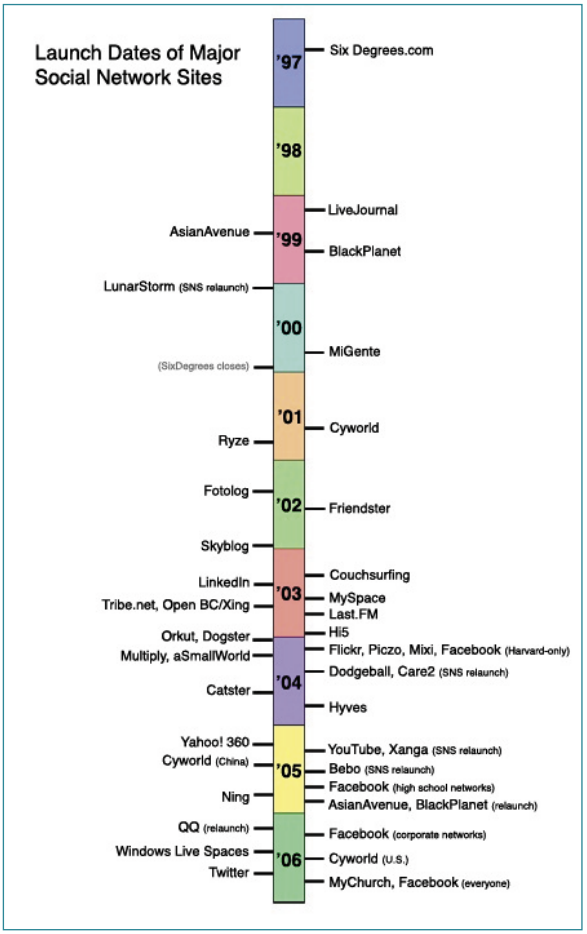

Figure 1. Timeline of the launch dates of many major social networking sites and dates when community sites re-launched with social networking site features (Boyd and Ellison, 2007).

is just a brief summary of the history of the social networks, which is important if we want to understand today's proliferation of social network websites and accordingly, the security risks of those networks, which is our main topic.

Security risks

Threat to privacy

'Many people may not be aware of the fact that their privacy has already been jeopardized and they are not taking steps to protect their personal information from being used by others' (Barnes, 2006). 'While the majority of people using these sites do not pose a threat, malicious people may be drawn to them because of the accessibility and amount of personal information that's available. The more information malicious people have about you, the easier it is for them to take advantage of you' (McDowell, 2011). People, who are ready to misuse your personal information, could do that in different ways. Social network users help them by revealing their personal information on their social network accounts. Since, social networks were originally established for fun, users do not even think that something bad can happen. Many social network websites include different applications which, in order to be installed and used, require giving the answers on, very often, personal details. Moreover, users who answer these questions, forward the applications and the question to friends on their friend list and that is how the attackers, in a very short period of time, receive a lot of personal information.

For example, revealing the name of your primary school or your teacher could be very dangerous. Why? In case you forget your password or user name, many Internet services allow you to chose a security question while creating your account. If you give the answer to it correctly, you can sign in without your username and password. These questions are, in most cases, the name of your school or the name of your first teacher. Accordingly, by revealing information concerning your primary school or the name of your teacher, attackers are able to enter the accounts you hold on much more important websites than social networks and misuse your information or take some confidential data. This is just one example of an indirect threat to privacy.

An example of a direct threat to privacy could be the following. By uploading your photos, for example, you could reveal your location. Or these photos could be misused for different purposes (advertising without your consent…). Furthermore, Facebook has taken action against people who were involved in its development; they realized that they were selling usernames and other data to dealers, who used them to determine precise target groups for dvertising material.

Threat to identity

There are several possible threats to identity concerning social networks, one of which is the so-called 'phishing'. 'Phishing is a form of social engineering in which an attacker attempts to fraudulently acquire sensitive information from a victim by impersonating a trustworthy third party. Phishing attacks today typically employ generalized "lures". For instance, a phisher misrepresenting himself as a large banking corporation or popular on-line auction site will have a reasonable yield, despite knowing little to nothing about the recipient (Jagatic *et al.,* 2005). 'Social networking sites are now a prime target of phishing, since the personal details in such sites can be used in identity theft. In late 2006 a computer worm took over pages on MySpace and altered links to direct surfers to websites designed to steal login details. Experiments show a success rate of over 70% for phishing attacks on social networks. The RapidShare file sharing site has been targeted by phishing to obtain a premium account, which removes speed caps on downloads, auto-removal of uploads, waits on downloads, and cooldown times between downloads' (Wikipedia, 2011d).

In practice, phishing functions like this: The user, whether through a message or some comment, follows the link which leads him or her to a website that is similar to some other website; for example, an official website of the bank. The fake website requires the user to type his or her e-mail address and password for using the bank's services. In that way, the attackers collect confidential data about the users and could cause them great damage. Fake profiles are also a threat to somebody's identity.

Threat to security

Concerning threats to security on social network websites, the most serious are so-called 'cyberstalking' and 'cyberbullying'. 'Cyberstalking is the use of the Internet or other electronic means to stalk or harass an individual, a group of individuals, or an organization. It may include false accusations, monitoring, making threats, identity theft, damage to data or equipment, the solicitation of minors for sex, or gathering information in order to harass' (Wikipedia, 2011e). Cyberbullying is 'the use of information and communication technologies to support deliberate, repeated, and hostile behavior by an individual or group, that is intended to harm others' (Puresight, ND). 'Cyber-bullying can be as simple as continuing to send e-mail to someone who has said they want no further contact with the sender, but it may also include threats, sexual remarks, pejorative labels (i.e., hate speech), ganging up on victims by making them the subject of ridicule in forums, and posting false statements as fact aimed at humiliation' (Wikipedia, 2011e).

How can you protect yourself?

Tip 1 – Read privacy policy rules

It is well known that most people do not read privacy policy rules relating social network websites. Some do not care about that, but the others do not even know that something like that exists. Strange, isn't it? 'We already know that people don't read online privacy policies and often (falsely) assume that *if* there's any such privacy policy it means their data is safe. There are, of course, even questions as to whether or not a privacy policy is even valid if no one reads it. Still, many consumer and privacy activists continue to act as if the privacy policy is a key aspect of online privacy. In fact, regulators in both the UK and the US seem to be admitting no one reads privacy policies, but demanding they are improved anyway. Specifically, a study done by regulators in the UK shows that 71% of people don't read privacy policies, but 62% want them clearer' (TechDirt, 2009).

If you buy something new, you always read the instructions. It should be the same with social

networks. These rules are important for two reasons. One is that privacy policy rules raise your awareness about social networks as public 'places'. The second is that these rules contain important tips on how to behave and how to customise your privacy settings on the social networks. Furthermore, these rules may contain information on how companies will use you personal information, about whether they will share or keep this information. 'A website's privacy policy tells you how information the site collects about you is used, shared and protected. On the basis of the information in the privacy policy, you should be able to decide whether or not to give information about yourself to the site' (GetNetWise, 2008).

Tip 2 – Select the information you post

It is important to know that, even if you customise your privacy settings so that only your friends can view your profile, you should only post information you don't mind being viewed by strangers. You cannot be sure that information you post will be safe in any case. It is impossible. Furthermore, remember that you cannot delete information once you post it. 'Once you publish something online, it is available to other people and to search engines. You can change or remove information after something has been published, but it is possible that someone has already seen the original version. Even if you try to remove the page(s) from the Internet, someone may have saved a copy of the page or used excerpts in another source. Some search engines "cache" copies of web pages; these cached copies may be available after a web page has been deleted or altered. Some web browsers may also maintain a cache of the web pages a user has visited, so the original version may be stored in a temporary file on the user's computer. Think about these implications before publishing information—once something is out there, you can't guarantee that you can completely remove it (McDowell *et al.*, 2005).

Tip 3 – Be cautious with strangers

'Identities can be elusive or ambiguous - Not only is it sometimes difficult to identify whether the "person" you are talking to is human, but human nature and behavior isn't predictable. People may lie about their identity, accounts may be compromised, users may forget to log out, or an account may be shared by multiple people. All of these things make it difficult to know who you're really talking to during a conversation' (McDowell and Householder, 2004).

Statistics – How people use the social networks

This is the survey conducted online by the researcher, which received 37 responses from people who actively use the Internet, in particular the social networks.

Question 1: *How old are you?*

< 18	0	0%
18 - 24	9	24%
25 - 34	18	49%
35 - 44	8	22%
> 45	2	5%

Question 2: *Your gender*

Female	15	41%
Male	22	59%

Question 3: *Did you ever search you personal name on the Internet and checked which information about you is available on it?*

Yes	0	0%
No	9	24%
I do not remember	18	49%

Question 4. *Is some of the following information about you available to others on the Internet? It is not a matter of whether you posted that information or somebody else.*

	Yes	No	I do not know	Responses	Total
Your e mail address	81%	19%	0%	37	10%
Your home address	5%	78%	16%	37	10%
Your home telephone number	14%	76%	11%	37	10%
Your cell phone number	29%	51%	20%	35	10%
Your employer/company you are working for	84%	16%	0%	37	10%
The political party you are voting for	5%	92%	3%	37	10%
Your photo	95%	5%	0%	37	10%
Your video	51%	32%	16%	37	10%
Groups and organizations you belong to	73%	19%	8%	37	10%
Your date of birth	56%	31%	14%	36	10%

Question 5: *In which way do you often post comments, questions and the information on the Internet?*

Using my personal name	21	57%
Using the nickname	13	35%
Anonymous	1	3%
I do not post them	2	5%

Question 6: *Do you care about how much information about you is available on the Internet?*

Yes I care	32	86%
No I do not care	4	11%
I did not think about that	1	3%

Question 7: *On which social network web site do you have a profile?*

Facebook	35	27%
MySpace	4	3%
LinkedIn	22	17%
Twitter	26	20%
Tagged	0	0%
Yahoo	11	8%
Flickr	10	8%
You Tube	14	11%
Hi5	3	2%
Other (explain in the text box below)	7	5%
I do not know	0	0%

ID	
3128451	orkut
3132543	TakingITGlobal
3180614	Xing
3206408	Ning & Buzz
3221174	diplointernetgovernance.org, Plaxo, Xing
3280013	Identi.ca, Softwarelivre.org
4219286	Xing, Plaxo, probably other abandoned accounts elsewhere

Question 8: *Is the information about you available on the social network websites visible for all people, not only for your friends?*

Yes	12	32%
No	23	62%
I do not know	2	5%

Question 9: *Do you believe that the companies which store the information about you available on the social networks, use that information in a responsible and a proper way?*

Yes I believe that they are using them in a responsible and a proper way	7	19%
No I think they are misusing them for the commercial purposes	21	57%
I do not know	9	24%

Question 10: *How do you use the social networks websites?*

	Yes	No	I do not know	Responses	Total
You change the privacy settings in order to limit the information you share with the others	97%	3%	0%	37	20%
You filtrate the news posted by your friends	56%	36%	8%	36	20%
You delete the people from your friends list/contact network	76%	22%	3%	37	20%
You delete your name from the photos you were tagged on	50%	42%	8%	36	20%
You delete the comments other people posted on your profile	33%	58%	8%	36	20%

Question 11: *Did yo ever try to delete some information about you on the social network web site?*

Yes	27	73%
No	7	19%
I do not remember	3	8%

Question 12: *Which kind of the material did you want to delete?*

	Yes	No	I do not know	Responses	Total
Photo or a video	73%	21%	6%	33	41%
Written material (comment or a blog post)	65%	29%	6%	31	38%
Other (explain in the box)	6%	47%	47%	17	21%

ID	
3236470	e-mails
3270253	tags
3280013	I once had a Facebook account, and I cancelled it (that is, I removed everything in it, so none of the options above fit my answer)

Question 13: *Do you think that the companies, like Facebook, Twitter, LiknedIn, are responsible for the security of your information available on their web sites?*

Yes	31	84%
No	5	14%
I do not know	1	3%

Question 14: *Do you write on your Facebook status information which refer to where are you or where you will be in the future?*

Yes	18	50%
No	17	47%
I do not know	1	3%

Question 15: *Before you add a new friend/contact do you check their profile and their references?*

Yes	26	70%
No	9	24%
I do not know	2	5%

REMEMBER: Social Networking requires responsibility of both the users and the social network providers.

References

1. Barnes SB (2006) A privacy paradox: Social Networking in the United States. *First Monday*. Available at http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/viewArticle/1394/1312%23note4 [accessed 15 April 2011].
2. Boyd DM and Ellison NB (2007) Social network sites: Definition, history, and scholarship. *Journal of Computer-Mediated Communication 13 (1)*. Available at http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html [accessed 15 April 2011].
3. GetNetWise (2008) How to read a privacy policy. Available at http://privacy.getnetwise.org/shopping/policy [accessed 15 April 2011].
4. Jagatic T, Johnson N, Jakobsson M and Menczer F (2005) *Social Phishing*. Available at http://www.indiana.edu/~phishing/social-network-experiment/phishing-preprint.pdf [accessed 15 April 2011].
5. McDowell M (2011) Staying safe on social network sites. US-CERT. Avaialble at http://www.us-cert.gov/cas/tips/ST06-003.html [accessed 15 April 2011].
6. McDowell M, Lytle M and Rafail J (2005) Guidelines for publishing information online. US-CERT. Available at http://www.us-cert.gov/cas/tips/ST05-013.html [accessed 15 April 2011].
7. McDowell M and Householder A (2004) Using instant messaging and chat rooms safely. Available at http://www.us-cert.gov/cas/tips/ST04-011.html [accessed 15 April 2011].
8. Nickson C (2009) the history of social networking. Digital Trends.com. Available at http://www.digitaltrends.com/features/the-history-of-social-networking/ [accessed 15 April 2011].
9. Puresight (ND) Cyberbullying. Avaialble at http://www.cyberbullying.org/ [accessed 15 April 2011].
10. TechDirect (2009) People don't read privacy policies…but want them to be clearer. Available at http://www.techdirt.com/articles/20090216/1803373786.shtml [accessed 15 April 2011].
11. Wikipedia (2011a) Social networks. Avialable at http://en.wikipedia.org/wiki/Social_network [accessed 15 April 2011].
12. Wikipedia (2011b) Bulletin Board System. Available at http://en.wikipedia.org/wiki/Bulletin_board_system [accessed 15 April 2011].
13. Wikipedia (2011c) Friendster. Available at http://en.wikipedia.org/wiki/Friendster [accessed 15 April 2011].
14. Wikipedia (2011d) Phishing. Available at http://en.wikipedia.org/wiki/Phishing [accessed 15 April 2011].
15. Wikipedia (2011e) Cyberstalking. Available at http://en.wikipedia.org/wiki/Cyberstalking [accessed 15 April 2011].
16. Wikipedia (2011f) Cyber-bullying. Available at: http://en.wikipedia.org/wiki/Cyber-bullying [accessed 15 April 2011].