SOCIAL NETWORKING SECURITY: DO CYPRIOT YOUTH REALLY CARE?

Despo Ktoridou, Ioanna Dionysiou,Ria Morphitou,
And Alexandros Klerides
University of Nicosia
Cyprus

Abstract

Social networking has been quickly adapted by the young population as the newest online trend, replacing or supplementing communications in the real world by diminishing barriers on physical location and time. Nevertheless, social networks are subject to all common security vulnerabilities of the web with their users being in even greater risk due to the implicit trust that governs these virtual communities. Besides the security concerns, privacy concerns also exist in social networks due to the vast amount of data that gets collected by the providers, allowing them to become digital big brothers. The aim of this paper is to investigate the user perceptions of the security and privacy risks when interacting with Social Networking Sites (SNS). A set of guidelines for social networking users to recognize the threats and to work knowledgeably is reported.

Introduction

Even though social networking emerged as organized virtual communities in the last few years, its drastically growing popularity is undisputed (Nielsen, 2009). SNS, such as Facebook, LinkedIn, MySpace, Orkut, and Twitter, attract millions of users everyday. Social networking has been quickly adapted by the young population as the newest online trend, while there are very strong indications of a rapid growth amongst older users as well. The popularity of social networks lies in the simple fact that they accommodate the exchange and sharing of information in an easy and intuitive manner for social, professional, and educational purposes. They even replace or supplement communications in the real world by diminishing barriers on physical location and time.

Social networks are subject to all common security vulnerabilities of the web with their users being in even greater risk due to the implicit trust that governs these virtual communities. For instance, users may show skepticism when receiving an email message that encourages them to click on a link or open an attachment, which is actually a malicious worm. However, they will click on such a link if it came from one of their social network connections. Besides the security concerns, privacy concerns also exist in social networks due to the vast amount of data that gets collected by the providers, allowing them to become digital big brothers. Personal and professional data could be exploited for a number of purposes, ranging from harming the system itself to increase economic profits via data mining techniques.

Social networking, despite the security and privacy issues, represents the next generation of the Internet. It is here to stay. The aim of this paper is to investigate the user perceptions of the security and privacy risks when interacting with SNS. To be more specific, the current study evaluates the perceptions of young Cypriots on social networking privacy issues, relative to the online activities offered by the various sites. A quantitative approach was employed for the purposes of this study, using questionnaires as the main method of data collection. Random sampling was used to select the participants. Cypriot youth aged 18-45 were the population of the study. The data collection process was conducted from October until December 2011. The paper discusses the data findings and provides a set of guidelines for social networking users to recognize the threats and to work knowledgeably.

Background

SNS popularity has been increasing amazingly. In particular, according to Facebook.com's statistics page, the site had 845 million monthly active users at the end of December 2011 and 483 million daily active users on average in December 2011(Facebook Statistics 2012). The advantage of these sites is that they can be used for professional networking business purposes, job search, public information on several issues or personal networking like reconnecting with friends from the past, making new friends, sharing with existing friends.

However, as with any novel tool or application, it is always important to consider seriously its security implications. Reviews of SNS usually suggest that the security of the most popular social networks ranges from very good to excellent. The evaluation criteria to assess the security of those sites include the following: support of privacy settings, block user feature, report spam feature, report abuse feature, and finally provision of safety tips. This perception of security gives uninformed users a false reassurance. As a matter of fact, SNS suffer from a number of security vulnerabilities that could be exploited intentionally and accidentally (Bonneau et al., 2009; Tubi et al., 2007). Facebook has suffered already cross-site scripting (XSS) exploits, in the form of session hijacking and fake login pages.

Security and privacy in social networks as perceived by the users has also being investigated (Esma et al., 2009; Karahasanovic et al., 2009; Putnman & Kolko, 2009). Users seem to expect the social network providers to support: trustworthy environment, privacy, anonymity, access control, and data usage transparency. In order to assess and evaluate the security model of a social network, a systematic approach is needed to define and assess its security attributes. The focus of this study is on the user, thus the evaluation of the security parameters is done from the user perspective and how s/he realizes and understands the security of a social network.

For our purposes, the security services required by a social networking site are the standard security services as defined by X.800: user authentication, data integrity, data confidentiality, data availability, and access control (Stallings, 2006). Specifically, the security services supported by a social network are the following:

- *Authentication:* one of the security services that it is provided by almost all social networks. It refers to the assurance that the communicating entity (user, provider, third party) is the one that it claims to be. In order to implement the authentication service, credentials such as username (or email) and password need to be supplied by the unauthenticated user, and upon verification the user is either authorized to log on or access is not granted.
- *Integrity:* refers to the assurance that the data has not been altered during its transmission to its intended destination.
- *Confidentiality:* refers to the disclosure of information or data to only authorized users.
- *Availability:* a system property where resources will be accessible and usable upon demand by an authorized system entity. Social networks suffer availability of service when denial of service attacks are launched due to either implementation vulnerabilities that get exploited or infected users being used as points of launching worms and Trojan viruses.
- *Access control and privacy*: the two most important pillars of social networks' security model. Users have strong expectations for privacy on SNS and they believe that it is the responsibility of the SNS providers to protect personal and user-generated content. The two terms are often used interchangeably as they are both associated with restricting access to user data.

Privacy, the ability to hide personal information from the system, is also a required service due to the vast volumes of data collected by both the provider and third parties.

Research Methodology

In order to investigate the user perceptions of the security and privacy risks when interacting with social networks, a survey was conducted among Cypriot university students. The survey questionnaire[1] focused on closed-ended questions that addressed factors involving most security services, such as authentication, confidentiality, integrity, access control, and privacy. It comprised of three sections. Part A collected demographic details, educational status, and Internet usage information for the respondent. Part B aimed in gathering more information regarding the online activities a responded was involved in. Part C examined the perceptions that a social network user has on matters involving security risks, profile data disclosure, authentication process, privacy settings, privacy, and confidentiality issues. At the end of the survey, the respondent was prompted to answer whether or not he/she will do anything different after taking the survey.

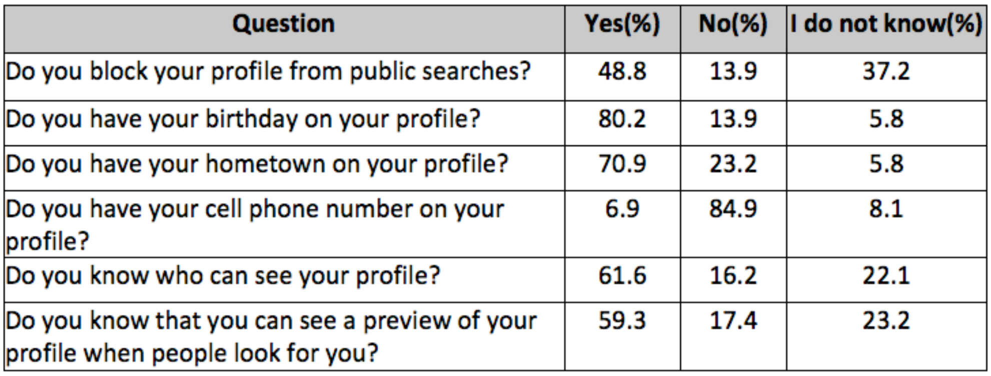
Questionnaires were collected during the period of October 2011 until December 2011, and the survey was conducted through personal interviews to assure the highest possible degree of accuracy for the received responses. The non-probability quota sampling method was employed with a sample of 109 users. After the completion of the survey, data from all the questionnaires were coded, compiled, tabulated and analyzed in accordance using SPSS (Statistical Package for Social Sciences) computer package.

Data Analysis

The social network users were 86 and the non-users of social networks were 23. Starting with the findings for the first two parts of the survey, a total of 74% of the participants fell in the 18-34 age group, 86% of the respondents were listed as university students studied either in Cyprus or abroad, and 73\% was using the Internet on daily basis. Surprisingly, all social network users had a Facebook account, and approximately 10% also had a Twitter account. It seems that Facebook is the dominant social networking site among Cypriot university students. When it comes to ways of accessing the social networking site, the most popular mean was using a laptop (45%), followed by a desktop (33%), and then a mobile phone (18%). The remaining users made use of tablets or another device.

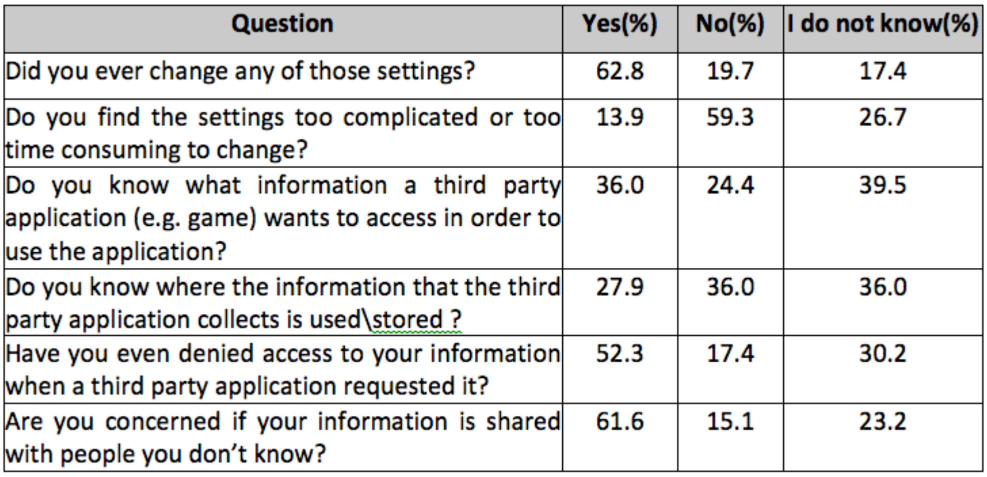
The majority of the respondents claimed to be aware of social security risks in general (68.6%). However it is alarming that 15.1% is not aware of such risks and a percentage of 16.2% does not even know what a security risk is. As a follow up question, 32.5% responded positively when asked if they use a public machine to logon in a networking site and do not uncheck the "keep me logged in" button. Furthermore, 41.8% use the same password to log on to various social networking sites.

Figure 1 shows the response distribution for the questions referring to profile information and Figure 2 lists the responses for the profile settings. 6.9% of the users post their cell phone number on their public profile that is viewable at least by their connections and/or strangers. Approximately 40% of the respondents are not aware who can view their profile and are not concerned who has access to their information. A percentage of 36% is aware of the information that third-party applications collect, and 27.9% even claims to know how the information is used and stored by such applications.



Question	Yes(%)	No(%)	I do not know(%)
Do you block your profile from public searches?	48.8	13.9	37.2
Do you have your birthday on your profile?	80.2	13.9	5.8
Do you have your hometown on your profile?	70.9	23.2	5.8
Do you have your cell phone number on your profile?	6.9	84.9	8.1
Do you know who can see your profile?	61.6	16.2	22.1
Do you know that you can see a preview of your profile when people look for you?	59.3	17.4	23.2

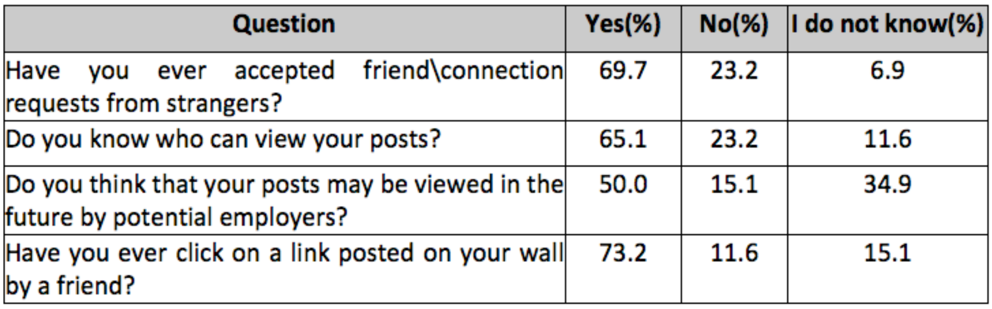
Figure 1. Response distribution for profile question set.



Question	Yes(%)	No(%)	I do not know(%)
Did you ever change any of those settings?	62.8	19.7	17.4
Do you find the settings too complicated or too time consuming to change?	13.9	59.3	26.7
Do you know what information a third party application (e.g. game) wants to access in order to use the application?	36.0	24.4	39.5
Do you know where the information that the third party application collects is used\stored ?	27.9	36.0	36.0
Have you even denied access to your information when a third party application requested it?	52.3	17.4	30.2
Are you concerned if your information is shared with people you don't know?	61.6	15.1	23.2

Figure 2. Response distribution for profile settings question set.

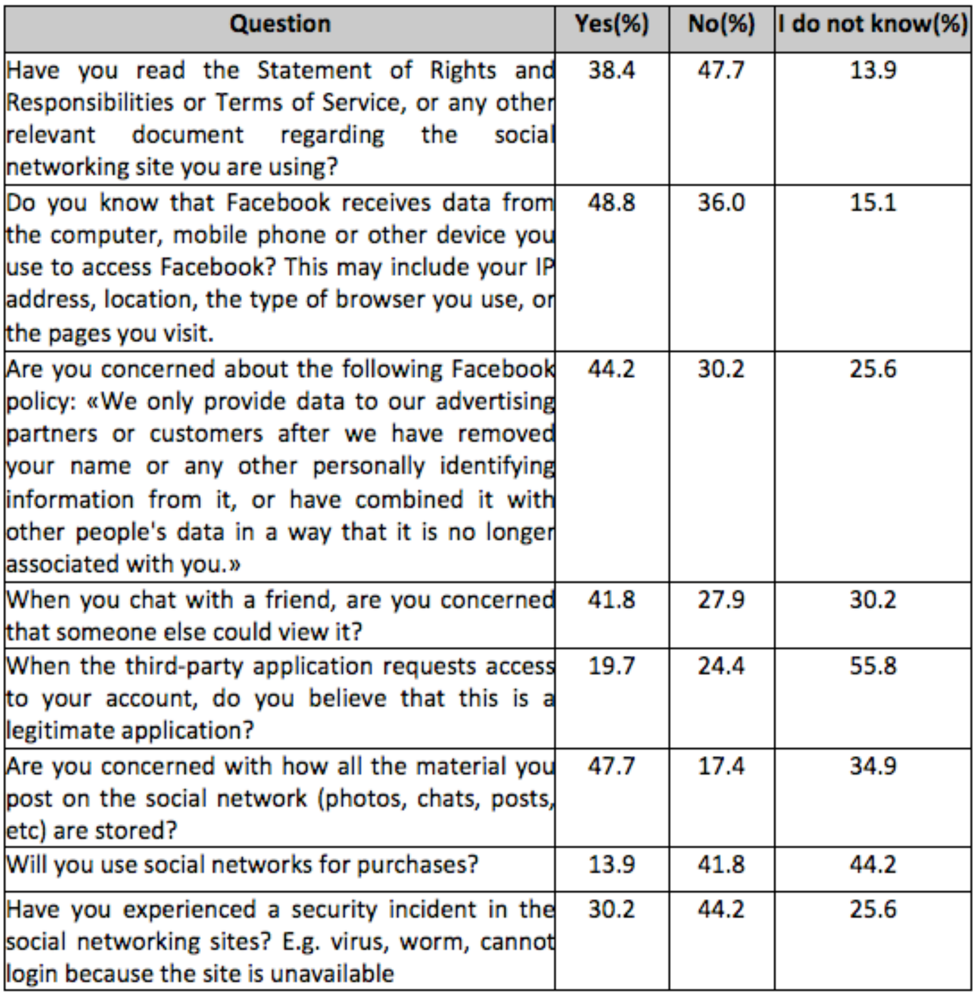
Figure 3 shows the response distribution for questions that involve a user's connections. An impressive 69.7% has accepted connection requests from strangers, showing that university students are willing to add into their circle users that they don't even know. Furthermore, 73.2% admitted that they click on a link posted by friends.



Question	Yes(%)	No(%)	I do not know(%)
Have you ever accepted friend\connection requests from strangers?	69.7	23.2	6.9
Do you know who can view your posts?	65.1	23.2	11.6
Do you think that your posts may be viewed in the future by potential employers?	50.0	15.1	34.9
Have you ever click on a link posted on your wall by a friend?	73.2	11.6	15.1

Figure 3. Response distribution for friends question set.

Finally, Figure 4 reflects the replies of the respondents on privacy and other security risks. Less than half of the users have read the terms of service regarding the social networking site they are using. In addition, only half of them are aware of the information that the social network provider is collecting. Almost one fifth of the users believed that a third-party application is a legitimate application.



Question	Yes(%)	No(%)	I do not know(%)
Have you read the Statement of Rights and Responsibilities or Terms of Service, or any other relevant document regarding the social networking site you are using?	38.4	47.7	13.9
Do you know that Facebook receives data from the computer, mobile phone or other device you use to access Facebook? This may include your IP address, location, the type of browser you use, or the pages you visit.	48.8	36.0	15.1
Are you concerned about the following Facebook policy: «We only provide data to our advertising partners or customers after we have removed your name or any other personally identifying information from it, or have combined it with other people's data in a way that it is no longer associated with you.»	44.2	30.2	25.6
When you chat with a friend, are you concerned that someone else could view it?	41.8	27.9	30.2
When the third-party application requests access to your account, do you believe that this is a legitimate application?	19.7	24.4	55.8
Are you concerned with how all the material you post on the social network (photos, chats, posts, etc) are stored?	47.7	17.4	34.9
Will you use social networks for purchases?	13.9	41.8	44.2
Have you experienced a security incident in the social networking sites? E.g. virus, worm, cannot login because the site is unavailable	30.2	44.2	25.6

Figure 4. Response distribution for security risks question asked.

To conclude, it seems that not all users are concerned about privacy, access control of their information, storage or distribution of their personal data, confidentiality, and authentication. Besides, only 11.6% responded positively when asked if they will do anything different after taking the survey. This is an indication of lack of security-awareness among the target population, which is not always due to ignorance but it could be intentional as well.

Conclusions and Recommendations

SNS has become a very popular means for people to communicate with family, friends and colleagues locally and internationally. In addition to the benefits from the collaborative approaches promoted by responsible use of SNS, concerns on information security and privacy still exist.

Results of the current study show that many of the respondents, even though they are aware of security and privacy risks, still create profiles, use computers in public places, do not know whether their profiles are blocked, have their dates of birth in their profiles, and are ignorant of how their personal information will be gathered, used and shared (they have not read the statements of rights and responsibilities). It is evident that the number of Internet users is increasing dramatically and it is difficult to find non-Internet users. SNS' popularity is growing dramatically, which is evidenced by the volume of users and the amount of personal information that is posted. Despite the numerous positive aspects of using SNS, it is also important for the users to understand the potential security risks and know what precautions to take to protect themselves and their information.

The nature of SNS encourages personal information posting, making users acknowledge security and privacy issues by intriguing them to provide more information about themselves and their life online than they would do with a person face-to-face. It is important for users to realize that posted information can be viewed by a broad audience, and could have implications. Clearly, security and privacy issues should be a priority for social networkers. Users need to be sufficiently informed by easily accessible/understandable privacy statements, especially young users soon to join the workforce; they should be aware of the potential consequences of posting inappropriate personal data on their SNS. Staying safe on a social networking service means recognizing security and privacy risks and working knowledgeably within a set of given guidelines: Attention must be given on what to reveal through a profile page, a bulletin board, an instant message or any other type of online communication that would led to exposure to unwanted visitors and/or identity stealing.

The Social Networking world is full of valuable and at the same time useless amounts of information. Users should treat any online information, news, stock exchange tips, lucky lotto numbers, gossip and many other cautiously. Anything users type online can always come back to them, they should always be careful and professional, and always think twice before typing. Social network services' privacy guidelines should be read and understood and in case the user disagrees with the terms he/she can choose to not to use the service.

Finally it can be concluded that social networking sites can be potentially useful tools for socializing only if users use them cautiously and think wisely before they take any action online.

Note

1. The actual questionnaire is available upon request.

References

Bonneau, J., Anderson, J., & Danezis, G. (2009). Prying data out of a social network. In *2009 Advances in Social Network Analysis and Mining* (pp. 33–40). IEEE Computer Society.

Esma A., Sebastien G., and Ai H. (2009). Upp: User privacy policy for SNS. In *Internet and Web Applications and Services, International Conference* (pp.267–272). IEEE Computer Society.

Facebook. (2012). Facebook statistics. Retrieved March 2, 2012 from http://newsroom.fb.com/content/default.aspx?NewsAreaId=22"

Karahasanovic A., BaeBrandtzg P., Vanattenhoven, J., Lievens B., Torben, N. K., & Pierson J. (2009). Ensuring trust, privacy, and etiquette in Web 2.0 applications. *Computer, 42*(6), 42–49.

Nielsen Company. (2009, March). Global faces and networked places: A Nielsen report on Social Networking's new global footprint. The Nielsen Company.

Putnman C. & Kolko B. (2009). Getting online but still living offline: The complex relationship of technology adoption and in-person social networks. In *2009 Advances in Social Network Analysis and Mining*, (pp 33–40). IEEE Computer Society.

Salkind, N. J. (2009). *Exploring research* (7th ed.). Upper Saddle River, NJ: Pearson.

Stallings, W. (2006). *Network security essentials: Applications and standards* (3rd ed.). Upper Saddle River, NJ: Pearson

Tubi, M., Puzis, P. & Elovici, Y. (2007) Deployment of dnids in social networks. In *2007 IEEE Intelligence and Security Informatics,* 59–65.