Online social networks and security of their users: an exploratory study of students at the Faculty of humanities and social sciences Zagreb

Radovan Vrana
Faculty of Humanities and Social Sciences
University of Zagreb
Ivana Lučića 3, 10000 Zagreb, Croatia
rvrana@ffzg.hr

Abstract. *The paper presents results from the research of students at the Faculty of humanities and social sciences in Zagreb, Croatia about their views and opinions about secure use of online social networks. The results indicate that most respondents are experiences users of online social networks; however, they rarely change passwords in their online profiles and most of them have never had any education about online security in general and methods of protection of personal data on online social networks. Luckily, most of them have never suffered from breaking into their profiles on online social networks.*

Keywords. Internet, online **s**ocial networks, security threats, user security, students

1 Introduction

In recent years online social networks have become a very popular global phenomenon. They changed ways in which people communicate and their ubiquitous availability "(…) has multiplied the number of interactions among users and changed their feelings about being networked" [20, 18]. An online social network is an internet service that serves as a platform for exchange of ideas, content, communication [1, 1036] and it facilitates interaction with long lost friends and family, colleagues, customers, learners etc. Online social networks "(...) are built on real-world social relationships and provide their users with a wide variety of virtual-interaction mechanisms." [2, 56]. Furthermore, online "(...) social networks provide a huge opportunity for implementing collaboration between users or different processes and actions undertaken by users" [3, 102] including teaching and research which are of great interest to students and researchers at the Croatian universities. According to the most recent online social networks statistics for 2012, "Sixty-seven percent of online adults say they use Facebook, 15 percent of online adults say they use Pinterest, 13 percent of online adults say they use Instagram, 6 percent of online adults say they use Tumblr, 16 percent of online adults say they use Twitter (and 20 percent of online adults say they use LinkedIn as of August 2012)." [4]. Because of their popularity online social networks are also vulnerable to different types of security threats. All users of online social networks are subject to security threats from family members, friends, acquaintances, colleagues, as well as from unknown people who are trying to contact them for different, often unknown reasons. As a result, security of users and their personal data on popular online social networks has been compromised significantly and repeatedly. This paper will present opinions and perceptions of students at the Faculty of Humanities and Social Sciences in Zagreb, Croatia about selected general and security aspects of use of online social networks.

2 Security issues on online social networks

The internet is extremely popular among younger generations, especially people that are 18 to 30 years old who are wired from birth [5, 36]. If one has to create a list of the most popular internet services today, he or she would place online social network high on the list of popularity. An online social network is "an online community of people with a common interest who use a Web site or other technologies to communicate with each other and share information, resources, etc." [6] "The primary focus of a social network service is to build and reflect a social structure of individuals or organizations which are connected by one or more specific types of interdependency, such as friendship, interests, disrelish, affection relationships, knowledge, and prestige or other social relations" [7, 190]. Online

social networks are more susceptible to software threats and attacks than other internet services mostly because they are attractive to many users [10]. By being popular, online social networks attract malevolent individuals and groups on the Internet who create problems for other online social networks users. As a result, use of online social networks could be potentially damaging to all generations of users of the Internet because of variety of security threats and attack methodologies which exist and continue to evolve as technology progresses globally [8, 92] and which now aim at online social networks.

Online social networks allow users to share activities, events, ideas and interests [7, 189] as well as other content which might be exposed to unknown persons as a result of a security breach. In recent years "Social networks have simply become another attack vector, whether for spreading malware, launching assaults on an individual's or company's reputation or creating impostor social networking sites that divert traffic away from the brand's legitimate sites." [9, 23]. Group of authors [2, 56] specified four categories of online social networks attacks: privacy breaches, viral marketing, network structural attacks, and malware attacks. Concrete examples of security attacks are: stalking, user privacy breaches, misuse of one's private data, reputation slander, online harassment and cyberbullying, sexual solicitation and exposure to problematic content. Indeed, there are many ways in which users can suffer damage on online social networks. Security attacks can be triggered by users who provide access to questionable content that could compromise users; who publish personal information about parents and family that could lead to identity theft; who choose online friends badly; who use weak passwords etc. [5]. One of the most frequent security threats is related to disclosure and theft of personal information of an online social network user. Personal information may include personal identifiable information like social security number (in Croatia, some other ID number like OIB), name and phone number which uniquely identify a person, home address, date of birth or former school he/she went or former company he/she has worked, religion, political view, type of disease or generated income [11, 848]. This type of data "(…) can easily be harvested by cyber-criminals without any technical know-how and with very little effort" [21, 9] and it can be mined for purposes of conducting phishing attacks [8, 94]. "The unauthorized disclosure of this type of data can result in serious consequences for an individual, ranging from social embarrassment and dissolution of relationships to the termination of insurance and employment contracts" [11, 848]. Online social networks users who demonstrate tendency for sharing their personal data too freely must know that "(...) there are at least two things that users need to understand if they are to properly exert a level of informed control over their social network contributions: 1.) the implications of sharing their information and 2.) the mechanisms available for restricting access if they wish to do so" [19, 14]. To avoid security incidents, users must be "(…) able to configure and control the access in their social networks" [19, 15]. Anonymity of users on online social networks is another problem. While it might seem attractive to some users to disguise their identity on online social networks to hide from parents or family who are also using online social networks, it also provides a great cover for malevolent individuals who send friend requests, Web site links or software applications to other users of online social networks pretending to be someone else. Normal users are usually unaware of possible security risks if they accept such friend requests or links that lead to other Web sites or software applications from individuals who sometimes pretend to be their friends and colleagues. These "(…) unwitting users can end up as fair game for phishing or even spear phishing scams by malicious individuals. A key problem in this context is that, by clicking on links sent from seemingly legitimate 'friends', they become vulnerable to malware infection from drive-by downloads" [18, 8]. As a measure of precaution, users of online social networks are usually advised not to leave personal information on an online social network [17], at least not detailed personal data which theft might lead to severe problems. However, users cannot protect themselves alone. Online social networks should also help their users by providing protection of users and their personal data in the following segments: user identity, user personal space and user communication with (selected) other users [12, 15]. In addition to intentional or unintentional disclosure of personal data, users of online social networks might suffer damage from using different applications written especially for use on a particular online social network. Applications on online social networks are used for marketing, file sharing, communication, and employee recruitment [15, 26]. Mansfield-Devine [13] warned about such online social networks applications (especially Facebook applications) that users readily accept not knowing that these applications can use malicious code to alter user's personal data and that these applications frequently have excessive permissions which enable them to parse user's personal data in the first place. For Sarrel [14] online social networks are useless toys that can contribute to violation of users own security.

We shouldn't also forget that the program code of online social networks itself is far from optimal and offers opportunities for creating malicious program code that would exploit deficiencies of that same program code.

Generally speaking, users of online social networks can protect themselves at least partially if not fully by stop doing the following: using a weak password, leaving full birth date in profile, overlooking privacy controls, posting names of family members in a caption, mentioning that user will be

away from home, letting search engine find user on Facebook (and other online social networks) and permitting children to use Facebook unsupervised [16]. Of course, best possible protection is common sense like in any case of use of information and communication technology and user provided content including sensitive personal information: "Education, or 'common sense' defense, is a key component in combating these cyber-threats" [21, 10]. Some online social networks like Facebook advance security of their users regularly, however, some measures can be very difficult to understand and to implement without making excessive restrictions in users' profiles.

The following part of the paper is focused on research of students at the Faculty of Humanities and Social Sciences (FHSS) in Zagreb, Croatia, and their views and opinions on different aspects of use of online social networks including security aspects.

4 Research

Students are one of the most distinctive categories of users of the Internet and online social networks as they belong to the already mentioned category of people between 18 and 30 years of age who are clearly frequent users of the Internet. In spite of the facts that confirmed the frequent use of online social networks by young generations, there is a constant lack of research of student population at the Croatian universities about their use of online social networks and other Internet services. This paper is an attempt to fill in this gap with focus on security aspects of use of online social networks by students at the FHSS, largest Faculty on the area of humanities and social sciences in Croatia. The results of the research should help in clarification of modes of use of online social networks by students in order to help them to use this popular Internet service for educational, professional and personal purposes more securely. This secure use would be presented to them through lectures. The purpose of this research is to get insight into use of online social networks by students at the FHSS. The aim of this research is to collect data about facts, views and opinions of students at the FHSS about security aspects of online social networks. A survey was chosen as the research method and a web questionnaire with 15 closed-type questions was chosen as a research tool. An e-mail invitation was sent to students' mailing list at the Faculty of Humanities and Social Sciences in Zagreb on March 6th 2013. Unfortunately, the students' mailing list doesn't include all the students at the FHSS as the ICT department at the FHSS decided to offer inclusion in the mailing list as an option to students rather than an obligation. As a result, this research will be limited to students who were willing to participate voluntarily. Future research will include paper based questionnaires to include students that are not included in the students' mailing list at the FHSS. The survey was closed at March 16th 2013 with total of 197 students who participated in the survey. While one might argue that this number of students is possibly low, it still indicates some important trends of use of the Internet in general and online social networks in particular by students at the FHSS.

5 Findings and discussion

This part of the paper will present results from the research. The results are given in form of tables to make their presentation and analysis easier.

Q1 How many different online social networks do you use at the moment? (N=197)

Table 1. Number of different online social networks used by the respondents

Value	Count	Percent %
None (Please, skip the rest of the questionnaire)	23	11,7%
One	94	47,7%
Two	47	23,9%
Three	21	10,7%
Four	7	3,6%
Five	2	1,0%
More than five	3	1,5%

Most respondents (47,7%) in the research use one online social network. These respondents are followed by 23,9% of the respondents who use two networks, and 21 respondents who use three online social networks. Both results are realistic since users (in general) are rarely able to participate intensively in work of several online social networks simultaneously. Another reason for a limited number of online social networks used by the respondents is popularity of certain online social networks. Simply put, users use online social networks that are popular among their friends, family members and colleagues. The popularity of online social networks rises and falls in time and users switch from one online social network to another in accordance with popularity of each of them.

11,7% respondents don't use any online social network which is not unusual since use of online social networks is sometimes very time consuming and users must see some benefits for them. Since the number of the respondents who don't use online social networks at all is greater than those who use three networks we can conclude that online social networks in present form didn't attract not entirely insignificant number of the respondents. Respondents who don't use any online social network were asked to skip all other questions in the questionnaire.

Q2 For how many years do you use online social networks for communication? (N=174)

Table 2. Experience in use of online social networks

Value	Count	Percent %
Less than 1 year	0	0,0%
1-2 years	14	8,1%
3-5 years	105	60,3%
6-8 years	48	27,6%
More than 8 years	7	4,0%

While online social networks exist for 15 years or more (depending on the source of historical overview of online social networks development), online social networks in the present form exist for little more than a decade. 60,3% of the respondents in this research have been using online social networks for 3-5 years and 27,6% of the respondents have been using online social networks for 6-8 years. Cumulatively, results in both categories cover more almost 90% of the respondents which is significant as the popularity of the most popular online social network such as Facebook started to rise considerably 5-6 years ago. This also means that participants in this research are not without experience in use of online social networks which most certainly contributes to their awareness of possible security issues that may appear while using their favorite online social networks. Simply put, more experience should mean more careful use of personal data and social networks in general. It is not always so.

Q3 What electronic devices do you use for access to online social network(s)? (multiple answers) (N=174)

Table 3. Electronic devices used to access to online social networks

Value	Count
Portable computer used only by me	127
Smartphone	101
Desktop PC shared with others	63
Desktop PC in the FHSS library	55
Desktop PC used only by me	50
Portable computer shared with others	42
Older generation mobile phone	39
Desktop PC in some public library	8
Tablet computer	8
Computer in an internet caffee	6
Kiosk computers in a public place (railroad station, airport)	5
Some other device	3
TV with Ethernet capability	2

Five electronic devices most frequently used to access online social networks are: portable computers used solely by respondents themselves, smartphones, desktop computers shared by others, desktop computers used in the library of the FHSS and desktop computers used solely by respondents themselves. The first two categories of electronic devices most frequently used to access online social networks suggest a need of the respondents to be mobile while using online social networks. High position of smartphones on the list of results was expected as their number in student population is increasing and as they are equipped with at least one online social network application (usually Facebook) at the time of purchase of the smartphone.

Q4 Select criteria important to you when making a decision whether to use online social networks. (multiple answers) (N=174)

Table 4. Criteria important for making a choice whether to use online social networks

Value	Count
My availability to friends	169
My availability to colleagues	120
My availability to some interest group	115
My availability to cousins	57
My availability to possible employer	38
My availability to professors at the faculty	26
My availability to other persons not listed here	19
My availability to all internet users	14
My availability to parents	12

Friends, colleagues and people we communicate with on the basis of our common interests are three most important criteria for the respondents in this research when they chose reasons to be member of particular online social networks. Inability to be next to their friends and other people made the respondents chose online social networks as a main medium for communication. Their decision to put friends on the top of the list of people whom they contact on online social networks is not important only from the cultural point of view but also from the security point of view. Many friends send each other different content including applications which might enable security breaches into personal profiles of online social network users as they often require permission of users to access their list of friends and to share it with the creators of applications.

Q5 Do you use your real name and surname for identification on online social network(s)? (N=174)

Table 5. Use of real name and surname for identification of online social network(s)

Value	Count	Percent %
Yes, every time	65	37,4%
Yes, sometimes	81	46,6%
No	28	16,1%

Almost 4/5 of the respondents use their real names (every time and sometimes) and surnames on online social networks to identify themselves to other users. While this is good if some other persons want to find them on online social networks it may also be a potential risk if they publish too much personal information that can be publicly viewed by almost anyone if online social network user is not careful enough. Some online social network users are using aliases instead of real names to communicate more freely with their friends and also to protect their true identity. Some other online social networks enforce use of real names and this decision might prevent some user from using their services.

Q6 How often do you change password for access to online social network(s)? (N=174)

Table 6. Online social network password change frequency

Value	Count	Percent %
Once a month	3	1,7%
Once in a three months	15	8,6%
Once in a six months	23	13,2%
Once a year	33	19,0%
Less than once a year	100	57,5%

More than a half of the respondents in this research change their password on an online social network less than once a year which is worrying. Another 1/5 of the respondents change their password once a year. Password change is part of a standard security routine in the global online environment and influences directly the level of security of a person's profile on an online social network. Users should change passwords more often and follow the recommendations for their complexity to avoid security breaches. Familiarity with such recommendations depends on users' knowledge about safe use of online social networks and the Internet in general.

Q7 Have you ever participated in some type of education about use of online social networks? (N=173)

Table 7. Participation in education about use of online social networks

Value	Count	Percent %
Yes	14	8,1%
No	159	91,9%

Over 90% of the respondents didn't participate in any type of education about use of online social networks. This result partially explains why there are so many security issues surrounding online social networks. Online social networks are frequently spoken and written about in terms of market value and number of users they attract but they are less frequently mentioned as good examples of internet services that care about informing their current and potential users about possible security issues. Some of them, such as Facebook do offer additional information about general use of their services as they introduce new functions, however, this appear to be insufficient.

Q8 Have you ever participated in some type of education about protection of your personal data on online social networks? (N=173)

Table 8. Participation in some type of education about protection of users' personal data on online social networks

Value	Count	Percent %
Yes	26	15,0%
No	147	85,0%

Results in this question are marginally better than results in the previous question. Only 15% of the respondents participated in education about methods of protection of their personal data on online social networks. Information and guidelines about safe use of online social networks that include protection of personal data are usually found on Web sites dedicated to secure use of the internet such as CERT (e.g. http://www.cert.hr in Croatia). Such information can be found often after security breaches already happen and when analyses done by security professional discover weak points of online social networks. For some online social networks users such information come too late because they personal identity might be already compromised if not stolen.

Q9 How often do you search for information on your own about new methods of protection of personal data on online social networks? (N=172)

Table 9. Frequency of search for new information about new methods of protection of personal data on online social networks

Value	Count	Percent %
Every day	4	2,3%
One a week	3	1,7%
Several times a month	6	3,5%
Once a month	8	4,7%
Once in three months	27	15,7%
Once in six months	36	20,9%
Less than once in six months	88	51,2%

The results in this question suggest that the respondents haven't put informing about new methods of protection of their personal data high on their lists of priorities. A little more than half of them (51,2%) search information resources on the internet on their own for information about new methods of protection of personal data once in six months which is inadequate when having in mind the speed of development of online social networks and frequency of discovered security breaches and number of personal data thefts. Generally speaking, users should be more careful (but not paranoid) and informed about these methods of protection as they are the ones who would benefit the most from this type of knowledge. Online social networks should also gently push information about security towards their users to keep them safe. Otherwise online social networks with most security problems will start losing users.

Q10 Have you ever falsified your personal data in your profile on an online social network to protect you identity? (N=174)

Table 10. Falsification of personal data in profile on an online social network to protect one's identity

Value	Count	Percent %
Yes	89	51,1%
No	85	48,9%

A little more than a half respondents (51,1%) falsified their personal data on online social networks to protect themselves against possible attackers. While this is a popular method among younger generations of online social network users, this type of behavior can be against a particular online social network policy. It may also result in blocking legitimate users of an online social network to find other people they seek for legitimate reasons. Advanced security functions on online social networks should prevent security problems that make users to fabricate basic facts about them and their lives and make them feel safer while using online social networks. Safety of personal data is not the only reason why online social network users fabricate their personal data. Hiding from parents, friends, colleagues and users can lead to opening successive user accounts on online social networks so users can use multiple accounts with different names in communication with family, friends, colleagues and other user categories. While some online social networks prohibit such practice, users don't care much about usage policies on particular online social networks and use multiple user accounts regularly as part of their social profile in society, among their friends etc.

Q11 Have you ever suffered from attempts for breaking into your profile on an online social network? (N=174)

Table 11. Suffrage from breaking into one's profile on an online social network.

Value	Count	Percent %
Never	141	81,0%
Seldom	29	16,7%
From time to time	4	2,3%
Often	0	0,0%
All the time	0	0,0%

While this is difficult to recognize clearly and without any doubt that a personal account on an online social network has been broken into, 2,3% of the respondents claimed that they suffered occasionally from such a criminal activity, while 16,7% of the respondents claimed that they suffered from the same activity seldom. Since this research didn't investigate into details of these incidents, there is no additional information that would explain why and how some users' personal accounts were broken into and with what consequences.

Q12 According to your estimation, what is the current degree of control over personal data on online social networks in general? (N=174)

Table 12. Current degree of control over personal data on online social networks

Value	Count	Percent %
Unsatisfactory	40	23,0%
Satisfactory	62	35,6%
Good	50	28,7%
Very good	18	10,3%
Excellent	4	2,3%

35,6% of the respondents in this research estimated that current degree of control over their personal data on online social networks is satisfactory; 28,7% of the respondents estimated the current degree of control as good and 23,0% of the respondents as unsatisfactory. Only 2,3% of the respondents found the current degree of control to be excellent. Online social networks users should have more power over personal data if social networks want to retain users. Most popular online social network Facebook makes regular efforts to improve control over personal data; however, this control must be simple enough to be used by users and powerful enough to brake by all others at the same time.

Q13 What is your attitude towards of existence of online social networks on the Internet? (N=172)

Table 13. Attitude towards of existence of online social networks on the Internet

Value	Count	Percent %
Positive	151	87,8%
Negative	21	12,2%

Almost 90% of the respondents have a positive attitude towards existence of online social networks

on the internet. Online social networks have many applications in our lives including education and business and it is important that they are accepted by users in general. This acceptance creates trust in online social networks and their capabilities to protect users from malevolent individuals and groups.

Q14 What is your attitude towards active participation in work of online social networks on the Internet? (N=173)

Table 14. Attitude towards active participation in work of online social networks on the Internet

Value	Count	Percent %
Positive	149	86,1%
Negative	24	13,9%

Significant percentage of the respondents (86,1%) demonstrated a positive attitude towards active participation in work of online social networks on the Internet which was expected. Since use of online social network is voluntary, this result is not surprising. Participants in this research were obviously highly motivated for use of online social networks which was expected since they are students and students tend to be regular users of online social networks. Additional research would be needed to clarify why 13,8% of the respondents don't have positive attitude towards use of online social networks but they still use them (see results in question no. 1)!

Q15 In your opinion, do online social networks offer enough protection of personal data to their users? (N=173)

Table 15. Protection of personal data to users of online social networks

Value	Count	Percent %
Yes	57	32,9%
No	116	67,1%

A little more than 2/3 of the respondents think that online social networks do not offer enough protection of personal data to their users and this should be changed. These users are aware of security issues which might lead to personal data theft and probably feel uneasy about possibilities that their data would be compromised in any way. Approximately 1/3 of the respondents feel safe enough to claim that online social networks offer enough protection of personal data to their users. As this percentage is rather low, more attention should be given to the improvement of safety of personal data on online social networks to make 90% of users feel safe about use of a particular online social network.

6 Conclusion

Online social networks are an important communication medium. As their popularity and number of active users increase they are becoming targets of malevolent individuals and groups who seek ways in which they would get control over users' profiles and their personal data. At present, there are many security issues related to online social networks such as: stalking, privacy breaches, misuse of one's private data, reputation slander, online harassment and cyberbullying, sexual solicitation and exposure to problematic content To continue use of online social networks safely users must be familiar with common safety measures. The research of students at the FHSS in Zagreb showed that 2/3 of the respondents are not satisfied with the current level of protection of their personal data i.e. their profiles on online social networks. Only few of them participated actively in education about safe use of online social networks and yet, they are using online social networks frequently. Their use of online social networks is limited mostly to one or two online social networks which enable them quality of use of online social networks services and greater focus on possible security issues while using these popular Internet services. Furthermore, they are able to monitor changes in online social network functions more thoroughly because they are better acquainted with functions and security features of one or two online social networks in comparison with functions of three, four or even more online social networks. As student tend to be mobile while using online social network, even greater number of them uses online social networks on portable devices (whether portable computers or mobile phones). While facilitating users' mobility and their availability to other users on online social networks could be recognized are good characteristics of most online social networks that are popular today, they also introduce new security issues such as use of applications that cannot be always trusted. Another problem is infrequent change of users' accounts passwords on online social networks. Students also seek information about protection measures for use of online social networks on their own far less frequently than they should. To protect themselves, students don't always use their real names on online social networks. Generally speaking, students are very keen on using online social networks and it seems that nothing will prevent them from doing that in future. However, they should invest more time in education about safe use of online social networks and apply common sense while accepting content from other people who are familiar to them and those who pretend to be their friends in order to protect themselves. Future research might include other groups of frequent users of online social networks to explore whether or not they follow the same pattern of use of online social networks as students at the Faculty of humanities and social sciences in Zagreb.

The future of online social networks is not certain in spite of the fact that they are currently central points of communication of many people and especially of younger generations on the Internet. Online social networks are popular, they have many purposes in our lives, but they are also virtual places where our personal integrity could be compromised easily if we forget that the Internet is an insecure place as much as it is a wonderful place.

References

[1] Beach, A; Gartrell, M; Han, R. Solutions to Security and Privacy Issues in Mobile Social Networking in International Conference on Computational Science and Engineering CSE '09, 1036-1042, Boulder, CO, USA, 2009.

[2] Gao, H; Hu, J; Huang, T; Wang, J; Chen, Y. Security Issues in Online Social Networks. Internet Computing, 15(4): 56-63, 2011.

[3] Ivan, I; Doinea, M. Social Networks Security. Journal of Applied Collaborative Systems, 1(2): 101-110. 2009.

[4] Ferenstein, G. Fresh Stats On Social Networks: Pinterest Catches Up With Twitter, Digital Divide Shrinks. http://techcrunch.com/2013/02/17/social-media-statistics-2012/ downloaded: February 22nd 2013.

[5] Gallo, E. The Young Adult: Financial Education, Social Networking, and Internet Security. Journal of financial planning, 24(10): 36-37, 2011.

[6] Social network. http://dictionary.reference.com/browse/social+network downloaded: February 22nd 2013.

[7] Hashimoto, GT; Rosa, PF; Filho, EL; Machado, JT. A Security Framework to Protect Against Social Networks Services Threats in 2010 Fifth International Conference on Systems and Networks Communications, 189-194, Uberlândia, Brazil, 2010.

[8] Mensch, S; Wilkie, LA. Information Security Activities of College Students: An Exploratory Study. Academic journal article from Academy of Information and Management Sciences Journal, 14(2): 91-115. 2011.

[9] Mitchell, RL. Scams, spams and shams. Computerworld, 43(31): 22-25, 2009.

[10] McClure, A. Friend of foe?. University Business, 13(10): 50-54, 2010.

[11] Ninggal, MIH; Abawajy, J. Attack vector analysis and privacy-preserving social network data publishing, in TRUSTCOM 2011 : International Conference on Trust, Security and Privacy in Computing and Communications, 847-852, Changsha, China, 2011.

[12] Zhang, C; Sun, J; Zhu, X; Fang, Y. Privacy and security for online social networks: challenges and opportunities. Network, 24(4): 13-18, 2010.

[13] Mansfield-Devine, S. Anti-social networking: exploiting the trusting environment of Web 2.0. Network Security 2008, 11: 4-7, 2008.

[14] Sarrel, MD. The biggest security threats right now. eWeek, 27(10): 16-19, 2010.

[15] Bahadur, G. Tips to Avoid Confidentiality Issues When Using Social Networking Media http://kraasecurity.com/itriskassessment/tag/gary-bahadur/ downloaded: February 22nd 2013.

[16] Social insecurity: What millions of online users don't know can hurt them. Consumer reports, 24-27, 2010. http://www.consumerreports.org/cro/magazine-archive/2010/june/electronics-computers/social-insecurity/overview/index.htm February 22nd 2013.

[17] Mediati, N. Social Network Privacy Settings Compared. PC World, 30(9): 37-38, 2012
.

[18] Everett, C. Social media: opportunity or risk? Computer Fraud & Security, 2010(6): pp- 8-10, 2010.

[19] Furnell, S. Social networks – access all areas? Computer Fraud & Security, 2011(5): pp: 14–19, 2011.

[20] Caviglionea, L; Coccolib M. Privacy problems with Web 2.0. Computer Fraud & Security, 2011(10): pp. 16–19, 2011.

[21] Parmar, B. Protecting against spear-phishing. Computer Fraud & Security, 2012(1): pp. 8–11, 2012.