

INFORMATION SECURITY AND PRIVACY AWARENESS IN ONLINE SOCIAL NETWORKS AMONG UTEM UNDERGRADUATE STUDENTS

Nur Fadzilah Othman¹, Rabiah Ahmad¹, Mariana Yusoff²

¹Faculty of Information Technology and Communication
Universiti Teknikal Malaysia Melaka, Malaysia

²Centre for Languages and Human Development
Universiti Teknikal Malaysia Melaka, Malaysia

Email: nurfadzilah132@gmail.com, rabiah@utem.edu.my,
mariana@utem.edu.my

ABSTRACT

The popularity of online social networks (OSNs) has increased dramatically in the recent years, counting more than one billion users in 2012. Hence, it leads to attraction of huge number of users. Nevertheless, OSNs not only implies a favorable effect on users but also impact an adverse effect on them. User create, administer and deal with the information and because of that, user are also a potential vulnerability. They often willingly, share personal identifying information about them, but do not have a clear idea of who accesses their private information or what portion of it really needs to be accessed. This paper observe the usage purpose and information disclosure in OSNs among undergraduates students in Universiti Technical Malaysia Malacca (UTeM). This paper will also explore level of information security and privacy awareness towards OSNs among them.

KEYWORDS *online social networks, security and privacy awareness, information disclosure*

1.0 INTRODUCTION

Recently, web-based Online Social Networks (OSNS), such as Facebook, Twitter and Myspace, have quickly emerged as a new internet killer-application. Boyd and Ellison, (2007) define social networking sites as web-based services that allow individuals to: (a) construct a public or semi-public profile within a bounded system, (b) articulate a list of other users with whom they share a connection, and (c) view and traverse their list of connections and those made by others within the system. OSNs are natural extensions of internet applications that establish relationships between users, such as email and instant messaging.

These OSNs offer attractive means of online social interactions and communications, but also raise privacy and security concerns. It is possible for somebody's profile to be connected to hundreds of peers directly, and thousands of others through the network's ties.

OSNs not only facilitate direct communication between users but also allow the users to post content that revolves around their profiles creating online personae that typically map to their real life personalities. In addition, OSNs explicitly expose a user's social contacts, enabling users to browse each other's social networks in search of common friends and interesting content (Gjoka, 2008).

This paper presents usage purpose, level of information security and privacy awareness and information disclosure in OSNs among undergraduates students in Universiti Technical Malaysia Malacca. The paper is organized into five sections. Following this introduction, the paper presents related literature, and then the research methodology employed in this study. The research results are then given, followed by the discussion and conclusion.

2.0. LITERATURE REVIEW

2.1. Usage Purpose and Information Disclosure

Along with technological development that occurs at this time, the use of online social network is seen as the main medium and become the most popular communication tool. According to Hewitt (2007), whenever an individual is born, it begins a journey of discovering the social world and culture it is embedded in. Gradually this environment becomes part of the individual's acting, as if it were a natural fact. Hence, the existence of OSNs provides new platform of acting, feeling expression and place to meet people and socialize. Boyd (2007) stated that, networked publics, as OSNs, can serve multiple purposes. as they can play a civic function, serving to gather people in a democracy. But they can also play a social role, enabling people to make sense of the world around them and understand their relationships to society. However, each individuals that react and engage in online communities and must have their own reason behind the movement and involvement in OSNs.

Many research have been made to understand why people participate or do not participate in OSNs. Results from other studies on similar social media platforms such as blogs show that bloggers ranked

pouring out feelings and connecting with people as the two most valued reasons for blogging (Liu et. all, 2007). Research by (Rheingold, 1993 ; Kim 2000) stressed the following motivational factors: 1) people with shared interests, 2) experiences and needs, 3) supportive and sociable relationships, 4) strong social feelings of belonging, and 5) a sense of shared identity. Besides, Brandtzaeg and Heim, (2009) exposed that the main motivation behind engaging in OSNs was to get in contact with new people, followed by keep in touch with friends and the third rank reason was general socializing.

In accordance with the concept of social networking site itself which is to connect and share with the people in your life, users willingly share their personal information, experiences, interaction and their everyday movement with the aim basically to connect and share with online friends. However, user wittingly reveal and disclose their information without realize that their private information had been exposed. Lenhart (2007) reports that 81 percent of parents and 79 percent of teens are not careful enough about giving out their personal information online. In a separate study of Facebook users done by Gross and Acquisty (2005), reveals that 71% of the Facebook users have the tendency to provide large amounts of sensitive personal information such as image and birth date in their profile that expose themselves to various kinds of security risks while Feizy (2007) in his article has revealed the fact that the users normally tend to reveal a variety of information including their name, age, gender, address, photos etc using their profile and some of them tend to hide, fabricate such information as well.

2.1 Information Security and Privacy Awareness

In information technology, security is the protection of information assets through the use of technology, processes, and training while awareness can be define as an individual's realization of the consequences of his or her actions and decisions. Information Security awareness is the degree of understanding of users about the importance of information security and their responsibilities and acts to exercise sufficient levels of information security control to protect organization's data and networks (Shaw *et.al.*, 2009).

OSNs also offer privacy setting to manage and control the privacy of user's status updates, photos and information. However, problems arise when user are not aware and do not use privacy settings that have been provided. It is proven in a research on Human Computer Interaction (HCI) by Wenday Mackay has shown that only a minimal percentage of users tend to change the default privacy preferences which are highly

permeable (Rosenblum, 2007). Other research conducted by (Acquisti & Gross, 2005) conclude that only a vanishingly small number of users change the (permissive) default privacy preferences. A year later, Acquisti and Gross (2006) found a results showing that OSNs users expressed high levels of concern for general privacy issues on Facebook, such as a stranger finding out where they live and the location and schedule of their classes, and a stranger learning their sexual orientation, name of their current partner, and their political affiliations. Tufekci (2008) found that concern about unwanted audiences had an impact on whether or not students revealed their real name in MySpace and whether or not students revealed their religious affiliation on MySpace and Facebook. Therefore, there may be an association between an individual's concern about unwanted audiences accessing his or her profile and the amount and types of information he or she chooses to reveal on Facebook.

Since online social networks are denser and more diverse than those offline, thousands of users may be classified as friends of friends of an individual and be able to access shared personal information (DiMicco & Millen, 2009). As Boyd (2007), describes that information shared online becomes persistent, searchable, replicable and subject to invisible audiences. While a relative majority of OSNs users are aware of the visibility of their profiles, a significant minority is not. The 'aware' group seems to rely on their own ability to control the information they publish as the preferred means of managing and addressing their own privacy concerns. Privacy in social networking sites must be taken into account. Especially when users' personal and sometimes private information may be sold to third parties without prior or proper permission (Jones & Soltren, 2005).

In a real experiment with users, Haddadi and Hui (2010) compared individuals' behavior with regard to friendship requests by using 40 fake identities of well known film stars and ordinary people on Facebook. The authors' results show that "usually users do not accept random friendship requests, but some aggressively search for celebrities, making a perfect case for spammers to form honeypots using such fake profiles".

3.0. METHODOLOGY

The questionnaire was developed to examine the usage purpose and type of information disclosure towards OSNs among undergraduates students from Universiti Teknikal Malaysia Melaka (UTeM). Besides,

the research will also explore level of information security and privacy awareness among them.

The study involves a number of students because the majority of social networking sites' membership are people in their teens and twenties (Huss, 2008). All participants have been selected because of their experiences or membership status with social networking sites. Data were collected from a randomly selected number of respondents using the stratified random sampling technique.

This survey consist of 3 part. Part 1 will tell about the demographic of respondent. Part 2 is about usage purpose and information disclosure while the final part is part 3 which is this part contain information about the information security and privacy awareness level among the respondent.

A total of 180 surveys were distributed in February 2012. Out of 152, 115 questionnaires were returned, yielding 75.7% response rate. In total, 107 surveys responses were recorded and used for statistical analysis. 8 respondent questionnaires were dropped due to incompleteness of the responses.

4.0. RESULTS

A. Demographic Profile

This study involve students of Universiti Teknikal Malaysia Melaka in the range of age 18 to 24 years old total of 77 students (72%) and 30 student (28%) in the range of age 25 to 34 years old.

They have been asked about their knowledge in internet usage and 16% of them stated they are very good, 53% of them is good while 33% have average level of knowledge in internet usage.

B. Usage Purpose and Information Disclosure

The results reveal that majority of respondents (71%) use OSNs as a place to spend their time. A large number of respondents (58%) use OSNs as a communication medium as well as a place to connect and find their old friends. 33% suggest that OSNs can be place for them to know and update their friends activities. 22% of the respondent admit that they use OSNs for looking and meet a new contact. The others reason for them to use OSNs because they use it for official use (18%) such as to creat an invitation event while there is also a small number

of respondent who used OSNs as a business platform (6.5%) for sales and promotions purposes.

The respondent have been asked about type of name they used in OSNs to allow other user recognized them. Most of them (50%) use part of their real names in OSNs while 31% of the respondent use their real name. The others, (19%) use nicknames as personal identification.

The results also expose type of image they used in order to other users recognize them. Most of them (42%) use their clear individual image as a profile picture. There are 31% respondent use images in group as a recognition and 27% do not put their own image.

Besides, the results discuss information they share in relation to the type of issue they update during updating status OSNs. Almost 66% of the respondent stated that most of issues they share in OSNs is their general knowledge followed by 41% of them share their emotion during updating status.

In this section, respondent also have been asked about type of personal information they share in OSNs and the result has shown in figure 1.

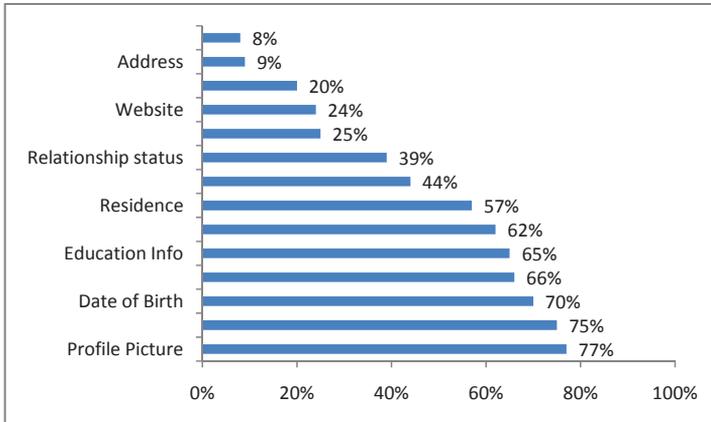


Figure 1: Personal information share in OSNs

The results of type of personal background they disclose in OSNs shows that 77% of the respondent show their profile picture in OSNs. 75% disclose their gender while 70% expose their date of birth in OSNs. It follows by exposing of real name (66%), education info (65%), family members (62%), residence (57%), work info (44%), relationship status (39%), email(25%), website (24%), partner name (20%), address (9%) and phone number (8.4%).

C. Information Security and Privacy Awareness

In this section, the respondents has to answer five questions to determine the level of information security and privacy awareness towards OSNs. Almost 78% of the respondents stated that they aware about the negative effects on the use of OSNs while 22% stated they are not aware the negative effect of OSNs. 80% of the respondents know who can access and see them, 20 % not sure who can access and see their profile while 16% do not know who can access their profile. 74% of the respondent use privacy setting and the remaining 26% do not use privacy setting in OSNs. Majority of the respondent (78%) do not read the OSNs terms of use, 3% not sure while 19% was read it. Although many respondent use privacy settings but the study shows that 75% of the respondent do not read privacy policy provided in OSNs. Only 22% of the respondent read the privacy policy and remaining 3% not sure about privacy policy of OSNs.

Table 1: Information Security and Privacy Awareness Level

Information Security and Privacy Awareness Level	No	Not Sure	Yes
User read OSNs privacy policy	80	3	24
User read OSNs terms and condition	83	3	21
User practice privacy setting in OSNs	38	0	69
User alert on who can access their profile	21	0	86
User aware on negative effect of OSNs	23	0	84

5.0. DISCUSSION

The first concern of this research seeks to investigate user’s usage purpose and information disclosure towards OSNs. The study reveals that most of the user use OSNs to spend their time and use OSNs as a communication media to connect with their old friends. OSNs was also a place for them to know and update their friends activities. From the result obtained, it can be conclude that the main factors that caused them to use the social networking site is an activities due to an engagement with friends. This results correspond to research done by Heim and Brandtzaeg, (2009) exposed that the main motivation behind engaging in OSNs was to get in contact with new people, followed by keep in touch with friends and the third rank reason was

general socializing. Based on the information they provide online, users expose themselves to various physical and cyber risks. More and more personal information disclosed and exposed, it can cause them to be at high risk of exposure to danger. The uncontrollable use of the name, image and information they shared during updating status on OSNs indirectly lead to the exposure of private and confidential personal information that should not be public. By disclosing personal information on OSNs users effectively place themselves at a greater risk for cyber and physical stalking, identity theft and surveillance (Gross & Acquisti, 2005).

The second concern regarding information security and privacy awareness in OSNs shows that the majority of OSNs members in our sample are know and aware about the negative effects of using OSNs. Most of them are aware of the visibility of their profiles to other users but a significant minority is not. It shows a different result conducted by Acquisti and Gross, (2006) revealed that most users were unaware or oblivious to privacy invading activities, as well as their risks, and had no idea of the extent to which one's online were exposed for others to view. Most users are aware of the negative effects of the use of OSNs have the ability to control information about themselves and concern who can access and view their profile. As if they also depend on themselves to control the dissemination of information on by managing and dealing with their own privacy concerns. Despite this concern, the study shows that users do not clearly understand terms and policies provided by OSNs service providers and it leads to misunderstanding of what information service providers share and release when users use OSNs.

6.0. LIMITATIONS AND CONCLUSION

The present study has a number of limitations. First, the findings are based on a small sample. Second, the results of the study can only be generalized to university students. Future research could seek to expand the present study by examining other user groups, such as high school or elementary school students and professionals, to see if their usage purpose, information disclosure and information security and privacy awareness behaviours differ from those of university students. Besides, most of the research related to OSNs was pioneered and conducted in western and developed countries. Therefore, it is a serious need for future research to be conducted in developing countries because dissimilar results may be obtained due to different levels of development, culture and lifestyle.

Overall, this study was important because it provided evidence that highly personal and sensitive information is being disclosed on OSNs.. The results of this study can be used to support the need for developing programs and indirectly reduce the risk towards user while using OSNs.

REFERENCES

- Acquisti, A. & Gross, R. (2006). Imagined communities: awareness, information sharing and privacy protection on the Facebook. In *Proceedings of the 6th Workshop on Privacy Enhancing Technologies*.
- Acquisti, A. (2004). Privacy in electronic commerce and the economics of immediate gratification. In: *Proceedings of the ACM Conference on Electronic Commerce (EC '04)*.
- Boyd, D. & Ellison, N. B. (2007). Social Network Sites: Definition, History and Scholarship," *Journal of Computer-Mediated Communication*, vol. 13, pp. 210-230.
- Boyd, D. (2003). Reflections on friendster, trust and intimacy. In: *Intimate (Ubiquitous) Computing Workshop - Ubicomp 2003*, October 12-15, Seattle, Washington, USA.
- Benevenuto, F. (2009). *Characterizing User Behavior in Online Social Networks Categories and Subject Descriptors*.
- Brandtzaeg, P.B., & Heim, J. (2009). Why people use social networking sites. *Proceedings of the HCI International*. (pp. 143–152).
- DiMicco, J. M. & Millen, D. R. (2007). Identity management: Multiple presentations of self in facebook. In *GROUP '07: Proceedings of the 2007 International ACM Conference on Supporting Group Work*, pages 383–386, New York, NY.
- Feizy, R. (2007). Evaluation of Identity on Online Social Networking: Myspace. In *18th Conference on Hypertext and Hypermedia (HT '07)*.
- Gross, R.. & Acquisti, A. (2005). Privacy and information revelation in online social networks. In: *Proceedings of the ACM CCS Workshop on Privacy in the Electronic Society (WPES '05)*.
- Gjoka, M. (2008). Poking Facebook: *Characterization of OSN Applications*, pp.1-6.
- Haddadi, H., Hui, P. & Brown, I. (2010). MobiAd: Private and Scalable Mobile Advertising, *ACM International Workshop on Mobility in the Evolving Internet Architecture*, Chicago.
- Hewitt, J. P. (2007). *Self and Society: a symbolic interactionist social psychology* (10th ed.). Boston (Mass.): Allyn and Bacon.

- Huss, S. (2008). Sight Speed Light, "SightSpeed Light Now Available on hi5," Available at: http://www.sightspeed.com/images/stories/Press_Releases/062008.pdf, [Accessed on 11 May 2012].
- Heim, S. , Crane, S. S., Böttcher, K., Krontiris, I. & Rannenber, K. (2011). Towards privacy-enhanced mobile communities-architecture, concepts and user trials. *The Journal of Systems and Software*.
- Haddadi, H. & Hui, P. (2010). To add or not to add: privacy and social honeypots. Proceedings of the ICC 2010: *IEEE International Conference on Communications*, 23-27 May, IEEE, Capetown, South Africa.
- Jones, H. & Soltren, J.H. (2005). Facebook: Threats to privacy. Student Paper. DOI <http://www.swiss.ai.mit.edu/6095/student-papers/fall05-papers/facebook.pdf>
- Kim H., Fang L. K., Lefevre, Tami A., Ave H., & Arbor A. (2010). A privacy recommendation wizard for users of social. *Electrical Engineering*, pages 630–632.
- Kim, A.J. (2000). *Community Building on the Web: Secret Strategies for Successful Online Communities*. Peachpit Press, Berkeley.
- Liu, S.H., Liao, H.L. & Zeng, Y.T.(2007). Why people blog: an Expectancy Theory analysis. *Issues in Information Systems Issues in Information Systems 8*, 232–237.
- Lenhart, A. and Madden, M. (2007). Teens, privacy and online social networks: How teens manage their online identities and personal information in the age of myspace.
- Rheingold, H. (1993). *The Virtual Community: Homesteading on the Electronic Frontier*. Addison-Wesley: Reading.
- Stutzman, F. D. (2006). An evaluation of identity-sharing behavior in social network communities. *International Digital Media and Arts Journal*, 3(1):10–18.
- Tang Y., Mao C., Lai H. & Zhu, J. (2009). Role Based Access Control for social network sites. *Joint Conferences on Pervasive Computing (JCPC)*, pages 389–394.
- Tufekci, Z. (2008). Can you see me now? Audience and disclosure regulation in online social network sites. *Bulletin of Science, Technology and Society*. 28, 20 (2008), 20-36.
- Young, A.L., Na, C. & Quan-haase, A., (2008). *Information Revelation and Internet Privacy Concerns on Social Network Sites: A Case Study of Facebook*, pp.265-273.