Security, Privacy Awareness vs. Utilization of Social Networks and Mobile Apps for Learning: Students' Preparedness

Daniel Koloseni

Department of Information Technology, The Institute of Finance Management

Dar-es – Salaam, Tanzania
koloseni@ifm.ac.tz

Abstract

The application of social networks and mobile apps for learning can improve learning process drastically in Higher learning Institutions as it offers tools and capabilities that creates flexible and convenient learning environment. But the utilization of social networks and mobile devices for learning is constrained among other things by fear of security and privacy of information shared. In order to investigate student's preparedness on security and privacy awareness in using social networks and mobile devices for learning, a descriptive research approach was employed. A judgmental sampling technique was used to select participants of the study. Based on the results of questionnaire and interviews we found that, generally students in higher learning institutions in Tanzania are short security knowledge and skills necessary to utilize social networks and mobile device for learning and therefore not ready to apply the same for learning. We propose measures to be done in order to make adoption of social networks and mobile devices for learning a success.

***Keywords**: Learning, Social Networks, Mobile Apps, Security, Privacy*

1. Introduction

Social networks and mobile devices offers learning capabilities that when harnessed properly can improve learning and education delivery [1]. Recent developments in ICT infrastructure, decrease in internet connection costs provide an opportunity for higher learning Institutions in Tanzania to use social networks as a secondary pedagogical tool for learning [2].Further, the establishment of Tanzania Computer Emergency and Response Team (TZ- CERT) and cyber security laws will provide both favorable learning environment and an impetus for using social networks and mobile devices for learning. A recent development in delivery of learning using social networks in Tanzania is seen in efforts made by The Institute of Adult Education through the Ministry of Education to deliver learning through mobile devices and social networks platforms and a number of locally and informally introduced social networking platform (wikis, blogs, discussion forum) and mobile applications in higher learning institutions.

The application of social networks in learning among other things is held back by fear of privacy and security of information shared [3]. In order to improve privacy and information security practices promoting good end security behavior is imperative [4]. One key step achieve that is through information security awareness assessment. It is, therefore, the intention of this paper to gauge the preparedness of students in relation to information security and privacy awareness when using social networks platforms and mobile apps for learning.

2. Security, Privacy and Trust in Social Networks and Mobile Apps

Information of social networks users is in jeopardy of being accessed and used by unauthorized users. Majority of social networks allow third-party applications to access and use information of social networks users without their permission [5] and [6]. Generally this practice is risking privacy of information of social networks users. Apart of that, many social networks do not enforce privacy settings or guarantee privacy of information of its users. User profiles of most of these social networks are by default visible to the public [7]. This puts new users and unskilled people into a trap of disclosing their information into wrong hands unknowingly.

Several studies have addressed the issue of security and privacy concerns of information circulating in social networks. For example, [8] examined privacy and disclosure of information in a social networking community while [9] developed a practical approach to preserve privacy in social networks against neighborhood attacks. Theoretical and practical analysis of vulnerability of social networks against the link of privacy attacks was provided by [10] . They [11] proposed an architecture called face Cloak that protects user's privacy by shielding user's personal information from the site and from unauthorized users. Privacy in online social networking sites was investigated in [12], while [7] researched on user's awareness of privacy on online social networking sites. Further, [5] and [13] studied information disclosure and internet privacy issues on social networking sites. Despite privacy and security concerns of user information, significance of security, privacy and trust are ignored by developers [14].

During the course of using social networks, students are vulnerable to several information security threats and privacy attacks such identity theft, social engineering and information loss. This may eventually discourage students to utilize social networks for learning. Security and privacy in education setting is crucial for sharing education related information in social networks as it builds trusts between participants. Building trust in social networks is a challenging issue because of the manner in which social networks are constructed. For example, methodologies used to create social networks such as neighboring matchmaker, friend of friend and word of mouth lacks trusted mechanisms for ensuring trust and privacy [14].With most of social networks developed under assumed trust between participants students are more vulnerable to disclose information to untrusted parties.

The application of smart phones, PDA's and tablets for learning is increasing among students in higher learning institutions worldwide. Most of new generation smart phones, PDA's and tablets have inbuilt capability to host mobile apps. Mobile apps provide fast, easy collaboration among participants. With increasing number of mobile application that does not require internet connection to access them, the likelihood of students to use them for learning is high.

Proliferation of educational mobile apps that can easily be obtained in online stores for free puts students into privacy and security risks such as identify theft and loss of information. Mobile apps with embedded malicious codes can steal student's information from the device and share to third party entities for financial gain or can be used for deformation purposes. Hence, ensuring security, privacy and trust among participants in education setting is important in order to cultivate usage of social networks and mobile apps for learning.

3. Research Approach

This study was conducted in higher learning institutions in Tanzania to investigate student's preparedness in security and privacy awareness aspects on utilization of social networks and mobile apps for learning. Participating higher learning Institutions were randomly selected from the lists of registered higher learning institutions from NACTE and TCU databases. Table 1 shows list of participating Institutions from both sides of Tanzania.

Population of the study consisted of undergraduate students only. Respondents from the study population were determined using judgmental sampling approach were by a researcher choose key informants that will suite the study. Hence, informants were selected based on their experience on using social networks and education mobile apps. Since this study is aimed at investigating student's security and privacy awareness when using social networks and mobile apps for learning therefore descriptive research approach was employed. This approach is suitable when collecting information about people's attitude, habits or any variety of education or social issue [15].

Data collection instruments used was interview and questionnaire. Myers suggest that interview is an excellent choice when gathering data related to people issues [16] therefore was deemed as appropriate for this study. Questionnaire was used to gather quantitative information regarding amount of disclosed information on social networks and precautionary measures taken by students when using social networks.

Table 1: List of participating Institutions

S/No	*Institution*
1	The Institute of Finance Management
2	University of Dar es Salaam
3	Sokoine University of Agriculture
4	Dar es Salaam Institute of Technology
5	Zanzibar State University
6	University of Bagamoyo

3.1 Research Design and Data collection Procedure

Interview questions and questionnaire were crafted to gauge student's security awareness through their actions when using social networks and mobile apps for learning. Specifically, interview questions and questionnaires focused on familiarity of possible threats, Awareness of f improper operation of social networks and reporting of security incidences, awareness on measures in handling personal sensitive information, cautious use social networks, cautious installation and upgrading of mobile applications.
Interviews were arranged beforehand through official letters. All interviews were conducted in respective higher learning institutions. Questionnaires were hand delivered to respondents by the researcher and collected after one week.

3.2 Data Analysis Plan and Execution

This study gathered both qualitative and quantitative data, therefore qualitative and quantitative data analysis methods were used. Qualitative data was sorted, grouped and coded to establish patterns and relationships to form five themes. The following themes were formed:

- Familiarity with possible online threats
- Awareness of outcomes of improper operation of social networks and reporting of security incidences
- Measures in handling personal sensitive information
- Precautions during accessing social networks
- Precautions during installation or upgrading of mobile apps

4. Findings

This section provides findings of the study. A total of 69 students participated in the study. Findings of the study were presented based on the above identified themes.

4.1 Familiarity With Possible Online Threats

Students were asked a series of questions to gauge their familiarity with possible online threats when using social networks. Knowledge about possible online threats is essential weapon that should be possessed by any internet user. Therefore it is essential that students should be familiar with possible threats in order to counter them. Our findings reveal that knowledge about online threats is not adequate among respondents (R1,R3,R4,R6,R7,R8,R11,R13,R16,R17,R18,R19,R20,R21,R22,R23,R24,R26,R27,R29,R30,R31,R32,R33,R34,R35,R36,R37,R38,R39,R41,R43,R45,R46,R47,R48,R49,R50,R51,R52,R53 and R54).
According to their response, the only possible online threat is virus. R4 was mostly concerned about the quality of internet and showed that is not concerned about other online threats apart from viruses.

'[…] when I log in into a social network or an online forum, my focus is to get access to the content that I am looking for. I know about viruses… but it is very difficult to enter my smart phone because I have never heard somebody been invaded by a virus in a mobile phone. […]' (Respondent R4)

However, respondents whose background is ICT, to some extent were knowledgeable about online threats. Most of them managed to mention possible online threats but were short of knowledge when it comes to methods and means to thwart them (R2,R5,R9,R10, R12,R14,R15,R25,R28,R40,R42 and R44).

4.2 Awareness of Improper Operation of Social Networks and Reporting of Security Incidences

Awareness of the outcome of improper operation of social networks and reporting of security incidences can help internet users to act precautionary when online. We gauged knowledge of respondents on range of aspects associated with improper operation of social networks and reporting of security incidences.
We asked them about what is allowed to be posted, what measures should be taken when somebody illegitimately get access to your password, username, full profile information including real name, date of birth, phone number, email, location, work place etc. We found that, most of respondents were unaware of what actions are improper when accessing social networks (R1,R2,R4,R7,R8,R10,R11,R12,R13,R15,R17,R18,R21, R22,R23,R26,R27,R30,R33,R36,R40,R41,R43,R45,R46, R49,R50,R53) They indicated that they don't bother

about their actions when using social networks. Some of respondents did admit that they had posted nasty comments in social networks (R17, R46).

Posting of nasty comments or abuse anybody is an offence. With regards to measures taken in reporting security related incidences, 83% admitted that they have never reported any security incidences and are not aware of means to do that. Few who reported security incidences, did it in unconvincing way (R15 and R43). As R15 epitomized,

'*When I found out that my social network account has been compromised, I will do the same like what I used to do with email accounts, open a new account and inform others that I have changed my email account'* (Respondent R15)

4.3 Measures in Handling Personal Sensitive Information

The study found that most of respondents are not knowledgeable enough in handling personal sensitive information when using social networks. Specifically we found 93% of respondents have their personal information filled in their Social Network profiles and out of that 93%, 66.7% respondents' information can be publicly accessed can be publicly accessible . This is similar to other studies on information privacy in social networks [5] and [17] , which also showed that most of respondents discloses their information on Social Networks. Personal information that is publicly accessible can be used by stalkers to victimize, bully, or used in other forms of crimes.
Table 2 shows the respondents' types of information disclosed on various social networking sites.

Table 2: Disclosure of information on social networks

Profile Information	Respondents (in %)
Real name	79.7
Date of Birth	77.2
Email	84.2
Phone number	97.5
Work place	39.2
Political view	14.2
Religion	9.4
Location	31.2

Information security and privacy policies play a vital role in safeguarding user's data when using computers or accessing the internet. Due to importance of security and privacy policies, we asked respondents a range of questions to determine the extent of their knowledge about it. We found that majority of respondents had enough understanding of the mentioned policies. This was clearly indicated by respondent R7, R8, R9, and R63.

'[…] *these policies provide a road on map what to do and how to do it in order to keep you safe when browsing […]* (Respondent R9).

Although most of respondents say they are aware of privacy and security policies available in social networking sites, in contrary we noticed that most of them did not bother to change the default privacy setting of their social networking accounts as directed in security policies. [18] suggest that this may be caused by user's fear of making bad configuration of their privacy settings, confusion since most of them are difficult to understand and its process may be taking a lot of time.

4.4 Precautions During Accessing Social Networks

Using internet services requires cautiousness attitude and prior knowledge of outcomes of internet user's actions. Therefore it is imperative that internet users should be act cautiously when accessing social networks because internet is a lawless zone, a playground of many undesirable activities and paradise of all sorts of criminals [19].To assess cautious behavior of respondents when accessing social network we asked respondents to list out measures taken by them to protect their personal information, the study found that, 88.9% of respondents use strong password to protect their account information, 48.6% restrict access to their profile and only 15.3% use up-to-date web browser as precautionary measure to keep their information secure. Response indicates that, respondents were highly prone to attacks and their behavior while working online is not good enough for them to use social networks as a learning platform and at the same time protecting themselves.

4.5 Precautions During Installation or Upgrading of Mobile Apps

Using and managing mobile apps is a challenge among mobile device users. Among challenges mobile device users face is management of upgrades, patches and fixes for the mobile apps. We therefore assessed their actions during management of mobile apps. We found that some respondents reported of difficulties in identifying and differentiating credible mobile apps for learning as exemplified by R29:

'*We find it difficult in identifying the right and credible source mobile app for learning and most of the time when I get a message to upgrade any of mobile apps in my smart phone, I do comply because I don't want to get deprived of service'* (Respondent R29).

To stay safe users should consider a parent company as a credible source of mobile apps. For example most of android apps are hosted in Google play app store which do not allow users to download mobile apps upgrades, fixes from third party market places, the same to App store. To be listed in App store a submitted application has to undergo a formal review process [20] which to some extent guarantee security and credibility of the mobile app. Further, users should consider protecting their smart phones, PDA's and tablets by installing anti viruses.

5. Discussion

In this section we discuss results of the study. Results are discussed in three different perspectives. First, we describe our observations from responses, second, we explain issues that may explain the observed situation and third we provide suggestions where possible.

Results indicate most of students in higher learning Institutions are not well equipped with knowledge of possible online threats and skills to combat the threats when using the internet and in particular when accessing social networks. There is a gap in knowledge on measures in handling personal sensitive information and cautious behavior when accessing social networks and installation or upgrading mobile apps. Most of the responses from the students can be explained based on personal traits and others can be a product of group based-values. Since respondents are from Higher learning Institutions part of results presented have reflection on the environment of the respondents.

With respect to knowledge lack of knowledge of possible online threats and skills to combat the threats when using social networks this can be explained as a product of inadequate security awareness training among the respondents. ICT is a new phenomenon and a new tool in education set up in Tanzania Higher learning Institutions which enroll most of the students with little knowledge of ICT or poor ICT background. Further, ICT was introduced as a subject recently and taught in few selected schools due lack of ICT facilities and qualified trainers [21]. Other issues that may explain the lack of knowledge of possible online threats and skills to combat the threats are outdated curriculums, lack of well trained teachers both in primary and secondary schools [22].

Social networks provide opportunity for users to post instantly, anywhere anytime users opinions, comments, media or notes. This opportunity when utilized correctly by students may enhance student's ability to grasp concepts learnt in classes. Possession of proper skills to use the social networks and mobile devices is therefore important to students [23]. Students should also be aware of legal issues regarding usage of social networks and use appropriate channels to report security incidences. For example, knowledge of what should be posted and what isn't is crucial when working online. In this study we found that most of the students have limited knowledge of what is permitted and what is forbidden to be posted in social networks, with some of respondents admitted in interviews that in one point or another they have posted nasty comments in social networks.

The newly established CERT and Cyber security laws will help to govern cyber- crime investigation, prosecution, reporting and prevention of security incidences. Further, institutional information security policies and guidelines can be used guide students on general usage of social networks. Development of Security cyber laws and establishment of TZ-CERT will create a promising and conducive environment for students to use social networks for learning.

On measures used by students to handle sensitive information, we found that 93% of respondents have their personal information filled in their Social Network profiles and out of that 93%, 66.7% respondents' information can be publicly accessed by anyone. This situation reveals lack of privacy concerns among users of Social Networks [5]. Lack of privacy concerns is further confirmed through interviews whereby respondents ignored to change privacy settings of their accounts as required by privacy and security policies in social networks. Most of social network are developed and loaded with privacy and security settings in order to ensure users privacy and security.

It is the discretion of the user to apply them or not to apply. Such kind of end user limitations should be addressed by cultivating an atmosphere of acting proactively to security incidences [24]. As far as online learning using social networks and mobile devices is concerned observance to privacy and security policies is inevitable.

Whilst accessing social networks for learning using mobile devices, students should make sure mobile devices are running up to date antivirus, browser and important OS security patches. Besnard and Arief suggests that most of security threats can be prevented by simply applying and running up to date security patches[25], this imply that using up to date antivirus and security patches can help to create a conducive environment for learning through social networks and mobile devices. In this study we revealed that most of the users are not taking precautionary measures before accessing social networks. This behavior jeopardizes their involvement in online learning through social networks.

6. Conclusion

The study aimed at assessing student's preparedness in terms of security and privacy awareness when using social networks and mobile devices for learning in Higher learning institutions in Tanzania.
In particular we investigated student's familiarity of possible threats, awareness of f improper operation of social networks and reporting of security incidences, awareness on measures in handling personal sensitive information, cautious use social networks, cautious installation and upgrading of mobile applications.

Based on the results of the study we conclude that, students in higher learning institutions they lack basic skills and knowledge on using social networks and mobile devices for learning and therefore not ready to engage themselves in using social networks and mobile devices for learning. Generally the study found that most of the students will be prone to different attacks. These attacks may eventually turn a social network into a very horrible place for learning to students and therefore discourage students and academic institutions to adopt social networks as an alternative pedagogical tool for learning. In addition to that, loss of privacy may cause economic losses and destruction of social image of individuals in the society [7].
Furthermore, loss of privacy may jeopardize physical security of social networking users as well. For example information obtained by unauthorized access (such location, real name, gender, work place, phone number, political view etc.) may be used for stalking, political parties campaigning, conmen and sexual predators just to mention a few.
E- Learning similar to traditional learning environment (classroom setting) needs to conducive enough to enable smooth learning to students. Unlike traditional learning environment, in e-learning environment, it is difficult to ensure security and privacy of information as these two factors depend on both technology and human factors. Principally, students are supposed to be the fore-runners in safeguarding their information on social networking sites.
However, in order to make this a success, higher learning institutions need to conduct information security and privacy awareness campaigns and incorporate information security awareness as a topic or sub topic in order prepare students on basic issues to adhere to when using social networks and mobile devices for learning. Lastly, to ensure privacy and security to students, higher learning institutions should lay down policies and regulations to ensure proper usage of Social Networks and mobile devices for learning.

References

[1] C. Lankshear and M. Knobel, *New Literacies: Everyday Practices And Social Learning: Everyday Practices and Social Learning*. McGraw-Hill International, 2011.

[2] D. Koloseni and Z. Omary, "Towards Using Social Networks and Internet-Enabled Mobile Devices for Learning: Students' Preparedness," in *Informatics Engineering and Information Science*, Springer, 2011, pp. 13–21.

[3] M. Conway, G. Maleko Munguatosha, P. Birevu Muyinda, and J. Thaddeus Lubega, "A social networked learning adoption model for higher education institutions in developing countries," *Horiz.*, vol. 19, no. 4, pp. 307–320, 2011.

[4] J. M. Stanton, K. R. Stam, P. Mastrangelo, and J. Jolton, "Analysis of end user security behaviors," 2004.

[5] R. Gross and A. Acquisti, "Information Revelation and Privacy in Online Social Networks (The Facebook case)," *Hum. Factors*, pp. 71–80, 2005.

[6] H. Lee, C. Chen, and C. Tien, "Android privacy 2 3," pp. 15–17, 2012.

[7] V. K. Tuunainen, O. Pitkänen, and M. Hovi, "Users' Awareness of Privacy on Online Social Networking sites-Case Facebook," *Bled 2009 Proc.*, p. 42, 2009.

[8] K. Strater and H. Richter, "Examining Privacy and Disclosure in a Social Networking Community."

[9] B. Zhou and J. Pei, "Preserving privacy in social networks against neighborhood attacks," in *Data Engineering, 2008. ICDE 2008. IEEE 24th International Conference on*, 2008, pp. 506–515.

[10] A. Korolova, R. Motwani, S. U. Nabar, and Y. Xu, “Link privacy in social networks,” in *Proceedings of the 17th ACM conference on Information and knowledge management*, 2008, pp. 289–298.

[11] W. Luo, Q. Xie, and U. Hengartner, “FaceCloak : An Architecture for User Privacy on Social Networking Sites.”

[12] R. Goettke and J. Christiana, “Privacy and online social networking websites,” *Comput. Sci. 199r Spec. Top. Comput. Sci. Comput. Soc. Priv. Technol.*, 2007.

[13] A. L. Young, C. Na, and A. Quan-haase, “Information Revelation and Internet Privacy Concerns on Social Network Sites : A Case Study of Facebook,” *Public Policy*, pp. 265–273, 2008.

[14] I. Liccardi, A. Ounnas, R. Pau, E. Massey, P. Kinnunen, S. Lewthwaite, M.-A. Midy, and C. Sarkar, “The role of social networks in students’ learning experiences,” *ACM SIGCSE Bulletin*, vol. 39, no. 4, ACM Press, pp. 224 –237, 2007.

[15] A. J. Orodho and D. K. Kombo, “Research methods,” *Nairobi Kenyatta Univ. Inst. Open Learn.*, 2002.

[16] M. D. Myers, *Qualitative research in business and management*. Sage, 2013.

[17] Z. Tufekci, “Can you see me now? Audience and disclosure regulation in online social network sites,” *Bull. Sci. Technol. Soc.*, vol. 28, no. 1, pp. 20–36, 2008.

[18] L. F. Cranor, P. Guduru, and M. Arjula, “User interfaces for privacy agents,” *ACM Trans. Comput. Interact.*, vol. 13, no. 2, pp. 135–178, 2006.

[19] G. Quirchmayr, “Selected legal issues related to Internet use,” in *Reliability, Quality and Safety of Software-Intensive Systems*, Springer, 1997, pp. 151–160.

[20] A. P. Felt and D. Wagner, *Phishing on mobile devices*. na, 2011.

[21] P. Swarts and E. M. Wachira, “Tanzania: ICT in education situational analysis,” *Glob. e-Schools Communities Initiat.*, 2010.

[22] M. Vesisenaho, J. Kemppainen, C. Islas, M. Tedre, and E. Sutinen, “Contextualizing ICT in Africa: The development of the CATI model in Tanzanian higher education,” *African J. Inf. Commun. Technol.*, vol. 2, no. 2, p. 22, 2006.

[23] D. Koloseni and Z. Omary, “Towards using Social Networks and Internet-enabled Mobile Devices for Learning : Students ’ Preparedness .,” 2011.

[24] M. Styles and T. Tryfonas, “Cultivating an Atmosphere of Proactive Computer Security to Mitigate Limited End-User Awareness.,” in *HAISA*, 2008, pp. 48–55.

[25] D. Besnard and B. Arief, “Computer security impaired by legitimate users,” *Computer. Security.*, vol. 23, no. 3, pp. 253–264, 2004.