Internet Security Awareness and Misuse of Social Networks of University Students

Dr.S.O.Akande

Centre for Educational Media Resource Studies
University of Ibadan
Emial: nyakand@yahoo.com   Phone: 08078768060

Abstract

The use of the Internet and social networking sites profitably to seek for information, for communication, social interaction and for learning and research purposes have been globally applauded by the society including the undergraduates. However, some undergraduates are not adequately informed about online safety measures they could adopt to prevent falling victims to online risks and anti- social behaviour. This study therefore attempts to investigate the level of students' awareness in security on the Internet and their level of involvement in online negative activities like bullying, fraud, impersonation and theft of information. The study adopted descriptive research design of the survey type. The sample size for the study was 300 undergraduates randomly selected from six departments in faculties of Education, Arts, and Science, University of Ibadan. Questionnaire was used as instrument for data collection. Data collected were analysed using frequency counts, mean scores and standard deviation. Pearson Product Moment Correlation was used to analyse data gathered on the research hypothesis. Findings of the study revealed that the students have high level of internet security awareness and low level of participation in online negative social activities. Based on the findings of the study, it was recommended that the University management through the University library and departments should ensure that their campaign on ethical use of the internet and social media continue by organizing more trainings, seminars and workshops to sustain the enlightenment of the students on profitable use of the media.

Key words: Internet, Security Awareness, Social Networking

Introduction

The Internet has come with inestimable privileges, potentials and profits. Communication with friends, seeking information, conducting online research and access to virtual libraries' collections with ease are just few of the immense benefits students can enjoy by using the global technology of Internet. The Internet is a public place where different categories of varied identities meet for different purposes. It is therefore not uncommon to have users that will mask their real identities by anonymity or pseudonymity. Wisdom calls for caution and security consciousness to escape the antics of unscrupulous entities that fake their identities while using the internet.

Studies like Tabatadze (2011); Sithira and Nguwi (2014) have shown that students represent a large percentage of population of Internet users who have suffered from the misuse and abuse of the social networking sites in online environment. Online risks and harms associated with social networking services are commonly reported in the literature. Kelly (2011) warned of the danger of not being security conscious by displaying too much information about oneself which may have serious implications on a person's privacy. According to him, majority of users who fail to alter their privacy setting while using the Facebook allowed a large number of unknown users to have access to their personal information. Little wonder that Student Internet Ethics and Acceptable Use Agreement (2012) for San Joaquin Country Office of Education Data Processing JPA prepared states that "when you are using the computer network and communicating with others in remote or even close locations, keep in mind that absolute privacy cannot be guaranteed in a network environment".

This study therefore attempts to investigate the level of students' security consciousness and their level of participation in negative online activities in the cyber environment. The study is important because libraries ought to be concerned about online safety of students. More so, understanding online behaviour and experiences of students on social media will guide the library management in policy formulation and implementation as regards the use of the Internet and web sites that allow interactive communications.

Insecurity in the cyberspace is a recent and new dimension of the global insecurity now threatening human peace and survival. It is no longer news that a lot of atrocities are perpetrated in the virtual environment in the form of Internet fraud, impersonation,

character assassination and bullying. An   explanation for these ugly happenings is probably because a large proportion of people of different demography now rely on the Internet for communication, seeking and sharing information. According to Tabatadze (2011), with the Internet on everyday part of our lives for communication, shopping, banking and education, the security awareness has never been more important as security threats become more complicated and we become more inter- connected. Perhaps, it is as a result of the increase in cybercrime that most universities have started to educate their students by offering courses, and embarking on several sensitization programmes to enlighten students on the dangers associated with the use of the Internet without being security conscious.

The cases of fraudulent practices, identity theft and inappropriate use of the Internet are subjects widely treated in the literature. Kotzanikolaou and Douligens (2008) reported that the security of information system is a serious issue because computer abuse is increasing everywhere.   Merkow and Breithaupt (2006) affirmed that although different control mechanisms are put in place by organizations to mitigate and preserve valuable electronic resources, data and information, yet the reality is that there is no absolute security. The perception of university of Ibadan students about privacy on the Internet can be a significant determinant of their online behaviour and how they will manage their privacy on the social networking sites. Sithira and Nguwi (2014) have written on youths and teenagers exposure to dangers associated with the use of social media. They confirmed that Internet fraud is serious and users who are not educated on the safety measures will fall victim to risks such as their personal and confidential information being stolen. Sims, Cheng and Teegen (1996) cited in Aliyu, Abdallah, Lasisi, Diyar, and Zeki (2011) asserted that unethical use of software such as privacy has been found to be common among students both undergraduates and graduates.

It is unfortunate that many students are not aware that unauthorized persons can access the information they share with their friends on social media. Privacy Rights Clearinghouse (2014) noted that the information shared with online contacts allows keeping in touch without much effort but many people besides friends and acquaintances are interested   in the information people post on social network. It is therefore implied that careless users of the social networking sites will expose themselves to untold online abuse. Naivety of students in handling their online privacy by volunteering personal information can make them suffer from online risk behaviour of those that lack understanding of ethical use of the social media.

Varnhagen and Husband (2011) remark on the report of the TLAT subcommittee on social media of the University of Alberta substantiates this claim when it states that : 'following the lead of industry and other universities, we need to develop clear and useful guidelines for appropriate communication with social media to protect the university community from online bullying and harassment. In a similar development, Furnell, Bryant and Phippen (2007) suggested that users' awareness of security threats matters and the education issue should be addressed by developing new models of engagement and awareness promotion. Mc Lean (1992); Spurling (1995) and Siponen (2000) all cited in Ryoo and Park (2011) also agree that increasing awareness in security is generally regarded as a positive trend.

This study on Internet security awareness is worth carrying out because it will generate empirical information on the online behavior of university of Ibadan students. The findings could also serve as basis for the formulation and implementation of Internet use policy in the university.

OBJECTIVES OF THE STUDY

The study is carried out with the following objectives in view:

1. Find out the years of experience of University of Ibadan students in using social media
2. Identify the level of students' awareness of internet security and negative online activities
3. Determine the level of participation of the students in negative online activities
4. Investigate the relationship between students' years of experience in using social media and level of awareness of internet security and negative online activities.

RESEARCH QUESTIONS

The study is guided by the following questions.

1. What are the years of experience of students' use of social media
2. What is the level of awareness of students about Internet security and negative online activities
3. What is the level of participation of students in negative online activities

HYPOTHESIS

The only hypothesis postulated for the study and tested at 0.05 level of significance states that:

There is no significant relationship between years of experience of students' use of social media and level of awareness of internet security and negative online activities.

RESEARCH METHODOLOGY

This study made use of the descriptive survey research design of the expost-facto type because the variables in the study have already occurred and were not manipulated in any way during the study. The undergraduates in Faculties of Education, Arts and Science, University of Ibadan constituted the population of the study. Using simple random sampling technique, Departments of Computer Science and Physics were selected in Faculty of Science; Departments of Philosophy and English were selected in Faculty of Arts while Departments of Library, Archival and Information Studies and Teacher Education were both selected in Faculty of Education. . From each of the departments sampled for the study, 50 students were randomly selected from   200 and 300 levels to form a sample size of 300 students.

The instrument for data collection was self- developed questionnaire divided into 3 sections. Section A contain items on bio-data of the students; section B is devoted to items related to awareness of the students about Internet security and negative online activities. It is a four point scale of 10 items to measure the level of awareness of the students. Section C is also a four point Likert type scale of 9 items developed to measure the level of involvement of students in negative online activities.

50 copies of the questionnaire were distributed to students in 200 and 300 levels in each of the six (6) departments to get a sample of 300 students used for the study. The questionnaire was distributed with the assistance of lecturers teaching 200 and 300 level courses. Out of the 300 copies distributed, 269 copies were filled and returned representing 89.7% return rate.

METHOD OF DATA ANALYSIS

The data collected was analyzed using the descriptive statistics of mean, frequency counts, percentage. The hypothesis was analysed by inferential statistics of Pearson Product Moment Correlation (PPMC)

RESULTS

Research question 1: What are the years of experience of students' use of social networking sites?

Table 1: Years of Experience in using social media.

Years	Frequency	Percentage %
1-3	60	22.3
4-6	137	50.9
7-9	47	17.5
10-12	16	5.9
Above 12	3	1.1
No response	6	2.2
	269	100

From Table 1, 60(22.3%) of the students had experience of 1-3 years of using social media; 137 (50.9%) between 4-6 years; 47(17.5%) between 7-9 years while only 3 (1.1%) of the students had used social media for more than 12 years. Table 1 shows that majority of the students, 137 (50.9%) have used the social media between 4-6 years.

Research question 2

What is the level of awareness of students about Internet security and negative online activities?

Table 2: Awareness of Students about Internet Security and Negative Online Activities

Items	VH	H	L	VL	Mean
Privacy	61 22.7 %	113 42.0%	63 23.4%	20 7.4%	2.84
Confidentiality	51	119	76	14	2.80

	19.0%	44.2%	28.3%	5.2%	
Copyright	57	101	72	23	2.76
	21.2%	37.5%	26.8%	8.6%	
Computer security	49	117	80	13	2.78
	18.2%	43.5%	29.7%	4.85%	
Computer ethics	60	113	73	9	2.88
	22.3%	42.0%	27.1%	3.3%	
Software privacy	69	84	66	24	2.81
	25.7%	31.2%	24.5%	8.9%	
Harassment	60	90	79	27	2.71
	22.3%	33.35%	29.4%	10.0%	
Hacking	79	87	63	29	2.84
	29.4%	32.3%	23.4%	10.8%	
Dissemination of rumour	103	76	48	29	2.99
	38.3%	18.3%	17.8%	10.8%	
Pornography	98	68	41	46	2.86
	36.4%	25.3%	15.7%	17.1%	

Weighted mean score = 2.83

NOTE VH = very high, H=high L= low,   VL=very low

Table 2 indicates the level of awareness of students about Internet security and negative online activities. Dissemination of rumour with (Mean = 2.99) was ranked highest in the mean score raking and was followed by computer ethics (mean=2.88); pornography (mean=2.86); privacy and hacking with mean scores = 2.84 each; software privacy (mean = 2.81). Harassment has the lowest mean score of 2.71 .The weighted mean score of 2.83 shows that the level of awareness of students about Internet security and negative online activities was high.

Research Question 3

What is the level of participation of students in negative online activities?

Table 3: Students' participation in Negative Online Activities

Items

Table 3: Students' Participation in Negative Online Activities

Items	VH	H	L	VL	Mean	S.I)
I participate in bullying, harassment and threatening on Social Networking Sites	40 14.9%	49 18.2%	46 17.17%	124 46%	2.02	1.14
I post questionable content on SNS	35 12.0%	89 33.1%	53 1.97%	79 29.4%	2.31	1.05
I use to gossip, spread rumour, and assassinate character on SNS	42 15.6%	57 21.2%	49 18.2%	108 46.1%	2.13	1.14
I post comments I would not like friends and close associate to see on SNS	21 7.8%	67 25.9%	63 23.4%	101 37.5%	2.03	1.00
I use to lie, cheat and gamble on SNS	30 11.2%	56 20.8%	44 16.4%	126 46.5%	1.96	1.09
I use foul language/ harmful communication on SNS	36 13.4%	52 19.3%	52 19.3%	114 42.4%	2.04	1.11
I participate in fraud and theft on SNS	40 14.9%	49 18.2%	31 11.5%	136 50.6%	1.97	1.16
I am used to hacking on SNS	34 12.6%	62 23.0%	38 14.1%	122 45.5%	2.03	1.12
I am fond of posting videos, pictures, and inaccurate information about people on SNS	46 17.1%	41 15.2%	36 13.4%	130 48.3%	2.01	1.19

Weighted mean score = 2.05

Table 3 shows the extent to which students participate in negative online activities. Looking at Table 3, 44(16.4%) of the students participating in lie, cheat and gamble reveals low level while 126(46.5%) of the students participation shows very low level. For fraud and theft, Table 3 reveals 31(11.5%) low and 136(50.6%) very low. Considering the level of participation generally, it could be seen that the level of participation of the students in negative online activities is low. The weighted mean score of 2.05 which is lower than the criterion mean of 2.50 also confirms low level of participation of students in negative online activities.

Hypothesis 1

There is no significant relationship between students' years of experience in using social networking sites and level of awareness of Internet security and negative online activities.

Table 4: Relationship between Years of Experience and Level of Awareness of Internet Security and Negative online activities.

Variable	n	X	S.D	r	P
Years of Experience using SNS	263	2.11	0.86	0.14	0.038
Awareness of Internet Security	226	28.23	5.14		

Correlation is significant at 0.05 level (2- tailed)

As presented in Table 4, data collected were statistically analyzed using Pearson correlation coefficient. As shown in Table 4, there is a significant positive relationship between students' years of experience in using social networking sites and   level of awareness about Internet Security and negative online activities (r = 0.14, p<0.05). .The hypothesis is thus rejected. This implies that for every increase in years of experience of students' usage of social networking sites, there is a corresponding improvement in their awareness of Internet security and negative online activities.

DISCUSSION OF FINDINGS

Research question 1: What are the years of experience of students' use of social networking sites?

The study revealed that majority of the students have spent 4-6 years in using social networking sites. With the launch of social networking sites reported in   Digital Trends (2014) that My space was launched in 2003; LinkedIn   in 2003; Face book 2004; Google+ 2007, it seems that majority of university of Ibadan students got to know about SNS at least 5 years after the first SNS was launched in 2003. This study has shown that only 16(5.9%) of the students surveyed had actually spent ten (10) years in using SNS especially sites like My space, LinkedIn   and Face book. The finding of this study does not support Boyd and Ellison (2007) which reported that the rise of social media sites as another platform on the internet has gained popularity over the last   decade.

Research question 2: What is the level of awareness of students about internet security and negative online activities?

This study indicated that the level of awareness of students about Internet security and negative online activities was high. The findings corroborates Aliyu, Abdallah, Lasisai, Diya and Zeki (2011) which reported satisfactory levels of awareness among the students of International Islamic University Malaysia (IIUM) about internet security and ethics.

Research question 3: What is the level of participation of students in negative online activities?

This study has shown low level of students' participation in negative online activities. The finding is at variance with Lack, Beck and Hoover (2009) which reported high levels of questionable unprofessional content and personal information being disclosed by medical students and residents while using social networks.

Hypothesis I: There is no significant relationship between years of experience of students' use of SNS and level of awareness of Internet security and negative online activities

The hypothesis has established that there is a simple linear relationship between years of experience of students' use of SNS and their awareness of Internet security and negative online activities. Exposure to the use of the internet and education on the use through courses taken on computer (Internet) security can actually promote awareness of Internet security. According to Aliyu et al (2011), students who attended courses on computer (Internet) security i.e. students who have been exposed to the use of Internet/social media have high level of awareness in comparison with students who didn't attend such courses. Similarly, the study of Ishak et.al (2012) on a survey on security awareness among social networking users in Malaysia has shown that respondents with higher educational background (well experienced /exposed in using SNS) are more aware on social networking security than respondents with lower educational background. The findings that a correlation exists between years of exposure of students' use of internet and level of awareness of Internet security is also in line with Ryoo and Park (2011) which reported that one may assume that more exposure to the Internet produces a technology - savvy user who can evade many potential threats from cyber criminals (i.e. more internet security conscious). Ryoo and Park (2011) also averred that the more time the users spend on the Internet, the more knowledgeable they became on security issues and they are more likely to practice security precautions.

Implications of Findings and Recommendations

The Internet is a social space where identity of users is very difficult to ascertain. The Internet shares some characteristics with the market where different categories of users with varied social, moral, educational, cognitive, cultural and religious backgrounds meet with different intentions and purpose. The concern to assist the students who are vulnerable and least aware of the dangers involved in using social networking sites without being security conscious is a strong motivation for this study. This study has revealed low level of students participation in negative online activities and high level of Internet security awareness. The risk behaviours like identity theft, cyber bullying, fraud, hacking, posting inaccurate information associated with social networking services to which students are daily exposed necessitate continuity in helping users staying safe online. A starting point is getting current information about the level of security awareness of the students while using the social networking sites which is the focus of this study. This information will serve as the springboard for instructional and training interventions on proper use of the internet backed with appropriate Internet use policy. University of Ibadan through the Kenneth Dike Library, could mount promotional programmes and campaigns focusing ethical use of the internet and the future dangers inherent in posting incriminating information on social networking sites. Courses on computer and internet education with emphasis on internet ethics and security should be made compulsory for all students especially for the first – year students in the university. The curriculum of The Use of Library aspects of GES 101 (a compulsory course for all first year students) should be reviewed to accommodate special trainings on ethical use of the internet and how to manage privacy on social networking sites. In conclusion, the library should demonstrate more concern by providing useful guidelines about online safety of students while using the social networking sites.

Conclusion

The study has shown a high level of awareness of internet security among the students in University of Ibadan. Nevertheless, a few students are still not aware of internet security and negative online activities perpetrated on the internet. As a result of the linear relationship established between years of experience in using social media and the level of awareness of Internet security, there is need for promotion of social media use in teaching and learning processes in the university to enhance student's online safety.

References

Aliyu, M,; Abdallah, N.A.O. ; Lasisi, N.A.;Diyar, D.; Zeki, A.M, 2011. Computer security and ethics awareness among IIUM student: An empirical study. http://www.academica.edu/46/383/computer. Retrieved 20 August, 2014

Boyd, D.M. & Ellison, N.B. 2007. Social network sites: Definition, history, and scholarship. Journal of Computer –Mediated communication, 13(1), 210-230

Furnell, S.M; Bryant, P; and Phippen, A.D. 2007.Assessing the security perception of personal Internet users. Computers and security, 26: 410-417

History of Social Networking, 2014. Digital trends staff. www.digital trends. Com/features/the - history-of-social networking. Retrieved 14th September, 2014.

Ishak, I., Sidi, F; Jabar, M.A. Sani, N.F.M, Mustapha, A; Supian, S.R. 2012. A survey on security awareness among social networking users in Malaysia. Australian Journal of Basic and Applied Sciences, 6 (12): 23-29.

Kelly, S. 2011. Identify at risk on Facebook BBC News. http://news .bbc.co.uk/1/hi/programmes/ click-online/7375772.stm. Retrieved 25 April, 2011

Kotzanikolaou, P and Douligenis, C. 2008. Computer network security: Basic background and current issues. http://citeseerxist.psuedu/view doc/download?doi. Retrieved 4th April, 2014

Lack, C., Beck, L; & Hoover, D. 2009. Use of social networking by undergraduate psychology major. Poster presented at the annual meeting of the Southeastern Psychological Association, New orleans, Louisiana, 2009.

Mclean, K. 1992. Information security awareness - selling the cause. In proceedings of the IFIPTCII, Eight International conference   on Information Security: IT security: The need for international cooperation, 179-193.

Merkow, M and Breithaupt, J. 2006. Information security principles and practices, New Jersey: Pearson Prentice Hall, Pp. 2

Privacy Rights Clearing House .2014. Fact sheet 35: Social Networking Privacy: How to be save, secure and social.

Ryoo, J. & Park, E. 2011. Internet security readiness : The influence of internet usage level and awareness on internet security readiness capital, skill, and actual uptake/ use of infrastructure. JCSE, 5(1), 33-50.

Sims, R.R; Cheng, H.K; and Teegen, H. 1996. Toward a profile of student software pirates. Journal of Business Ethics,   15 (8) : 839-849.

Siponen, M.T. 2000. Conceptual foundation for organizational information security awareness. Information Management and Computer security 8,(1): 31-41

Sithira, V and Nguwi, Yok-Yen. 2014. A study on the adolescent online security issues. International Journal of Multidisciplinary and Current Research. http://ijmcr.com/wp-content/uploads/2014/06/paper. Retrieved 20th August, 2014.

Spurling, P. 1995. Promoting security awareness and commitment. Information Management and Computer security, 3(2) : 20-26

Student Internet ethnics and acceptable use agreement 2012. http :www.lincolnhigh.org/userfiles/server-5796227 Retrieved 20th August, 2014

Tabatadze, D. 2011. Internet security awareness program in Geogia, funded by ISOC Community Grants Program: Final Report. https:www.inter society.org/sites/default/files/pdf. Retrieve 20th August, 2014.

Varnhagen, C. and Husband, A. 2011. Social media: Use and Usefulness at the University H Alberta. Report of the TLAT subcommittee on social media. http://www.ctl.ualberta.ca/sites/defaul/social/20 Media. Retrieved July 17, 2014