

Dangers in Online Social Networks: An Assessment of Awareness and Exposure of Tertiary Institution Students in Oyo, Oyo State, Nigeria.

OLUWOLE FOLARANMI ALABI (Ph.D)

Department of Communication and Media Studies

Faculty of Social & Management Sciences

Ajayi Crowther University, Oyo State

Nigeria

E-mail: of.alabi@acu.edu.ng, olualabi9@gmail.com

Abstract

Debates on social networking sites have been centered on security issues and on whether the benefits outweigh the dangers. The preponderance of social network dangers notwithstanding, many young adults, particularly tertiary institution students in Nigeria have continued the risky practice of posting online personal information that online predators could use against them. Can this risky practice be ascribed to lack of awareness of the inherent dangers, and; to what extent do the students make themselves vulnerable? These are the issues investigated in this study. This survey has all students in the four tertiary institutions in Oyo town, Oyo State Nigeria as its target population. Purposive sampling was employed in selecting 200 students (fifty (50) students per institution) to participate in the study. Students' Awareness and Exposure to Social Network Site Dangers Questionnaire ($r=0.81$) was administered on all the subjects. Findings show that majority of the participants are aware (89%) of the dangers in online social networking. Both male and female respondents are 'very much aware' of the possibility of addiction to social networking, social imposters and online scammers, identity theft and invasion of privacy as potential dangers. This awareness seems not to have positive effect on how students expose themselves to the dangers as many of them remain vulnerable by posting personal information such as birthday (96%), e-mail address (87.5%), information about their institutions (81.5%), posting original recent photographs (74.5%), information about country and cities of residence (66%), phone numbers (66%) and relationship status (64%) on their social network pages. The study recommends urgent media education among these students to stop the trend and forestall attendant dangers.

Key words: Social network sites, dangers, awareness, exposure

Introduction

Social network sites are platforms for building social networks or social relations among people who share interest, activities, backgrounds or real life connections. Notably, the advent of social networks such as Facebook, Myspace, LinkedIn etc has attracted millions of users globally. According to Boyd and Ellison (2007)., social network sites are web-based services that allow individuals to construct a public or semi-public profile within a bounded system, articulate a list of other users with whom they share a connection, and view and traverse their list of connections and those made by others within the system. As noted by Heverly (2008), social networking has

actually reinvented communication that takes place in a more flexible way in which children share advice and support with peers. Virtually every age demographic is using online social network (OSN) sites to communicate with others, and the medium is extremely popular and widely used to exchange social capital by students (Pempek, Yermolayeva and Calvert, 2009).

In the recent time, debates on social network sites have centred on security issue and whether the benefits outweigh the dangers. Proponents argue that social network sites promote increased communication with friends and family, familiarized more people with valuable computer skills, and allow contact with people from around the world, unfortunately, it has equally become a valuable tool in the hand of evil people who take advantage of innocent and undiscerning users who routinely post information on their OSN pages that they ordinarily wouldn't share with a stranger on the street. Such information include: birthday, phone number, e-mail address, home address, family details, intimate thought, mood status, relationship status and lots of pictures (Tania Dworjan,2011).

Social network sites are employed to close the communication gap in an ever evolving society. These media are for people to connect and relate with one another notwithstanding the long distance. Some of the sites attract so many people. Most of the users are not aware of the need for online protection. Unfortunately, the sites have become tools for online scammers, fraudsters and other criminal-minded people to cheat unsuspecting and innocent individuals. The dangers are real and numerous. Among others are: Social imposters, identity theft, cyber-bullying, scam, social defamation, addiction tendency and invasion of privacy.

The preponderance of social media site dangers notwithstanding, many young adults, particularly, tertiary institution students appear to continue with the risky practice of posting personal information that make them susceptible to the dangers. Can this risky behavior be ascribed to lack of awareness of the dangers? To what extent do the young people expose themselves to the dangers? These are critical questions that necessitated this inquiry.

Literature Review

The threat and dangers on social network sites are numerous. Among them is the threat by social imposters. The social imposters are the people who pretend on the Internet to be what in reality they are not. These people give deceptive information about their true identity so as to fit into the high class category of life. Con artists can also be found under this category because they do not operate with their true identity. Facebook, Twitter and other social platforms are easy way of making friends, either known or unknown. On such platforms, all that social imposters do is to simply cover up their real identity, lie to be another person in order to deceive unsuspecting people and lure them into illicit deals. Many young people have fallen victim of forced sex while many have lost valuable possessions to these online robbers.

Users' identities can be easily accessed by criminals' network who may pose as friendly applications to steal user's personal identifying information. It appears many people are yet to realize the fact that information posted on social network is not safe. Just like the normal robbery operations where robbers hijack a person's car and use it to cover up their identity in a robbery operation, so is the case of social network robbers. The only difference in this case is that social identity thieves do not apply force; they only perfect their operations by carefully harvesting information and pictures that have been voluntarily submitted by the users of social network

sites. Unfortunately, many of the users of social network sites, and of course the owners too, do the least to prevent the intruders. In a report on 23 Internet service companies, the watchdog organization -- Privacy International, charged Facebook with severe privacy flaws and put it on the second category for “substantial and comprehensive privacy threat” (A Race to the Bottom, 2007)

Cyber bullying is another potential danger faced by social network users. Cyber bullying is more prevalent in America. It has always been a major issue among teens, especially high school peer groups. The concept of cyber bullying involves harassment, picking-on, threatening or causing harm using the Internet. (Natalie Gillian, 2011). Because of the cloak of anonymity under which online bullies often operate, the medium makes it easy to harass both young people and adults in schools, at work places or in any other social and non-social contexts. Most of the bullies post harmful and awful information, pictures and video about a person in order to embarrass the individual or to settle a score with the individual.

Scammers or con artists constitute another threat to social network users. According to Natalie Gilliam (2011) scam can come in different ways ranging from solicitation for help, donation or assistance to outright scheme to defraud, using intimate information that had been provided inadvertently by the users in his or her user’s profile on the site for people to see. Many people post much information about their jobs or business on Facebook and other sites for people to see. Through this the con artists are able to get detailed information to use on specific users to scam them of their possessions. Again, making new friends through social media makes many users mindless of the kind of friends they add and information they share without paying attention to the consequences of their actions. Countless number of people have fallen victim of social network scam. In Nigeria, the case of Cynthia, a young undergraduate of Nassarawa State University who was lured into an hotel at Amuwo-odofin in Lagos, dispossessed of her belongings, raped and killed by the people she met on Facebook is highly instructive.

Social defamation is another potential threat posed by the social network sites. With the fast speed, vast ability of the Internet and the ability to sent instant messages on the social network services, news spread faster than wildfire. It is easy to lose one’s reputation in real life through misconduct but at least, the news is only within the territory in which it occurred, but on the Internet, it is not so. On the Internet, such damage to one’s reputation goes viral. Unfortunately, what goes on the Internet stays on the Internet. With the rise in social media, it takes less than five minutes to damage user’s reputation. Posting inappropriate comment on the various social network sites can cause ruination to user’s reputation.

The danger of possible addiction to social network is another potential danger facing online social network users. All over the world, a lot of young people are already tending toward more online friends than offline friends. According to Jenney Cheerver (2010), most people find it preferable to stay online or relate with people online than in real life situation. People tend to spend more hours chatting with friends online than making use of the Internet for other profitable and rewarding purposes. Many students who are already entrapped in the web of social network addiction spend more time social networking online than they spend time extracting information from their books.

The implication of social network sites for personal privacy is another budding issue. With the invasion of social networking sites, account users tend to provide all sorts of information about

themselves (background information, job information, likes, dislikes etc.) without the protection of such private and valuable information through privacy control. Online predators can use such online information by manipulating user's picture, setting up fake users' profiles and publicizing embarrassing private information to harass individuals.

Statement of Problem

With the advent of the Internet, more ways of communicating with friends, staying in touch with long- lost pals, and meeting new people have abound. Instant messaging services and chat rooms are being created as tools to bridge the communication gap between long distance relationships and its being used frequently because of its ability to deliver messages instantly and cheaply. People sign out for these social networking services (Facebook, LinkedIn, Myspace, Twitter etc.) beginning with opening of account which requires them to publish information about themselves and their innermost thoughts, without realizing that it is not only their friends who are viewing the information but also anyone with access to the Internet, including online predators and sex offenders.

The danger inherent in making friends with total strangers on social network is really great. The social network services which was created to bring love and friendship to the world has become an instrument through which evil people and fraudsters lure unsuspecting victims to their death and ruination. Many people have argued about the dangers in engaging in social networking online. Such people believe that there is nothing wrong with it as it helps build social capital and enhances business opportunities all over the world. Others simply frown at the wisdom behind making friends and visiting total strangers and sharing personal information with them or engaging in all sorts of business transactions with them.

News of sundry crime such as identity theft, people falling victim of fraudsters and other kinds of criminality is all over the media and the knowledge of such crimes may save one from being a victim. But, some young people are in the habit of not keeping themselves informed about the happenings in the country while some are up-to-date with the current happenings in the society and also take caution in their online activities.

In view of the inherent dangers in social networking online and because research efforts hitherto have been focused primarily on the effect of online social networking, the inherent dangers and not much has been done in the area of measuring users level of awareness as well as their exposure to the inherent dangers through risky practices in Nigeria, it becomes necessary to carry out this study.

Research Questions

To effectively address the focus of this investigation, the study will provide answer to the following research questions:

RQ1: Are the tertiary institution students in Oyo aware of the danger on social networking sites?

RQ2: What is the level of awareness of the SNS dangers by male students?

RQ3: What is the level of awareness of the SNS dangers by female students?

RQ4: Are the tertiary institution students exposing themselves to the dangers?

Method

The study made use of survey research design. The targeted population for the investigation includes students in the four tertiary institutions in Oyo town, Oyo State, Nigeria. Samples were drawn from Emmanuel Alayande College of Education (formerly known as Oyo State College of Education), Federal College of Education (Special), Ajayi Crowther University and the Federal School of Surveying in Oyo.

Purposive sampling procedure was employed in selecting samples from each of the four institutions. A subject only qualified for selection after meeting the criteria for selection: (i) the subject must have a current and active page on a social network site, (ii) He or she must have operated the page for at least two years, (iii) He or she must have at least fifty persons in his or her network of friends. The criteria are aimed at ensuring that only students that are active social network users are selected. Initially three hundred (300) copies of the research questionnaire were administered in each of the institutions. From the copies of the questionnaire properly filled and returned, fifty copies from respondents who met the stipulated criteria were selected from each of the institutions. A total of 200 copies (fifty from each of the institutions) were subjected to statistical analysis.

Students Awareness and Exposure to Social Network Dangers Questionnaire ($r = 0.81$) was administered on all respondents. SAESNSQ was developed and validated by the researcher. The data collection instrument consists of three sections, A, B and C. Section A of the questionnaire consists of items focusing on the demographics of the respondents and on whether they have account with social network or not, the length of usage and the number of people on their networks. Section B contains twenty (20) main items in ‘Yes’ or ‘No’ response format. The third section, section C is however structured in four-point Likert Scale format of “Very much aware”, “Aware”, “Partially aware” and “Not aware”. Data generated with the instrument were analyzed with frequency counts and percentage. The results were presented in tables.

Results

RQ 1: Are tertiary institution students in Oyo aware of the dangers in online Social networking?

Table 1: General awareness of the dangers in online social networking among students

Awareness	Frequency	Percentage
Yes	178	89.0%
No	22	11.0%
Total	200	100.0

Table 1 shows the general of awareness of tertiary institution students on the dangers inherent in online social network sites. 178 students, amounting to 89% as against 11% of the sampled students claimed to be aware of the dangers on social network sites. By implication, it can be concluded many of the respondents, by extension, majority of the tertiary institution students in Oyo have full awareness of the possible dangers.

RQ 2: What is the level of awareness of each of the SNS danger by male students?

Table 2: Level of awareness of SNS dangers among male students

Possible Dangers	Very much aware		Aware		Partially aware		Not aware	
	Freq	%	Freq	%	Freq	%	Freq	%
Identity theft	55	59.1%	25	26.9%	9	9.7%	4	4.3%
Addiction tendency	58	62.4%	28	30.1%	7	7.6%	0	0%
Invasion of privacy	39	42%	37	39.8%	14	15.1%	3	3.2%
Social impostors	49	52.7%	29	31.2%	10	10.8%	5	5.4%
Scammers/ Con artist	49	52.7%	32	34.4%	9	9.7%	3	3.3%
Cyber bullying	32	34.4%	34	36.6%	15	16.1%	15	16.1%
Social defamation	28	30.1%	36	38.7%	17	18.3%	12	12.9%
Job background check	32	34.4%	16	17.2%	16	17.2%	29	31.2%

Table 2 explores the level of awareness of male students on the specific online SNS dangers. Of all the dangers, possibility of getting addicted was rated highest (Very much aware =62.4%) followed by identity theft (59.1%), Scammers, and Social impostors were the same (52.7%) by the respondents.

RQ 3: What is the level of awareness of each of the SNS danger by female students?

Table 3: Level of awareness of SNS dangers among female students

Possible Dangers	Very much aware		Aware		Partially aware		Not aware	
	Freq	%	Freq	%	Freq	%	Freq	%
Identity theft	66	61.7%	35	32.7%	5	4.7%	1	0.9%
Addiction tendency	73	68.2%	27	25.2%	3	2.8%	4	3.7%
Invasion of privacy	53	49.5%	39	36.4%	8	7.5%	7	6.5%
Social impostors	72	67.3%	21	19.6%	9	8.4%	5	4.6%
Scammers/ Con artist	65	60.7%	30	28.0%	6	5.6%	6	5.6%
Cyber bullying	28	26.2%	39	36.4%	24	22.4%	16	15%
Social defamation	34	31.8%	40	37.4%	21	19.6%	12	11.2%
Job background check	37	34.5%	30	28.0%	18	16.8%	22	20.6%

Table 3 examines the level of female students awareness of each of the online social network dangers. The table shows that 68.2% of the sampled female students rated possibility of addiction as the highest (Very much aware) followed by ‘Social impostors’ (67.3%), ‘identity theft’(61.9%), ‘Scammers’(60.7%) and ‘invasion of privacy’(49.5%). This results show that other potential dangers of SNS such as ‘Cyber bullying’, ‘social defamation’ and ‘Job background check’ are not acknowledged as serious dangers.

RQ 4; Are the students exposing themselves to the dangers on SNS through risky practice?

Table 4: Students exposure to SNS dangers

Information volunteered on SNS by students	Yes		No	
	Freq	%	Freq	%
Birthday	192	96.0%	8	4%
E-mail	175	87.5%	25	12.5%
Country and city of residence	149	74.5%	51	25.5%
Institutions attended	170	85%	30	15%
Faculty/ department	95	47.5%	105	52.5%
Recent pictures	183	91.5%	17	8.5%
Family background information	42	21%	158	79%
Relationship status	128	64%	72	36%
Phone number	132	66%	68	34%
House address	64	32%	136	68%

Table 4 shows the types of personal information of the respondents that they voluntarily allow everybody to have access to on their SNS pages. As much as 96% of the respondents have their birthday on SNS pages, 91.5% have their original and recent pictures on SNS pages, 87.5% make their e-mail addresses accessible on SNS pages, 85% make information about their department and faculty available, 74.5% make available information on their country and city of residence. While 66% make available their personal phone numbers, 64% post their relationship status on their SNS pages.

Discussion of findings

As evident in the results above, majority of the tertiary institution students in Oyo are fully aware of the dangers on social network sites. Findings from both male and female respondents show a level of uniformity. Among all dangers, Addiction tendency, social imposters, identity theft and scammers are the highly rated dangers. The high level of awareness of these dangers could be ascribed to the fact that they are the most rampant dangers into which many online social network users fall in Nigeria. Other dangers such as such as cyber bullying, invasion of privacy, and social defamation are more common in in the Western world that in Nigeria and of course, in Africa in general.

Conversely to the findings on awareness is the fact that, in spite of the high level of awareness, many students remain vulnerable to the dangers because of the amount of personal information they make available on their SNS pages. As clearly shown in table four, vital personal information of respondents such as their date of birth, e-mail address, recent pictures, city and country of residence, and in fact, phone numbers are accessible on their SNS pages. These are all information usable to online predators in tracking down potential victims. This finding confirms the submission of Tania Dworjan (2011) that social network sites users routinely post information on their Facebook and other social network sites pages that ordinarily they would not share with a stranger on the street. Unfortunately, even though most users would not share the vital personal information with the stranger on the street, they unwittingly share the same with everybody anywhere in the world who needs such information to fester sinister intention.

Conclusion and Recommendation

The findings of this inquiry have shown that although tertiary institution students in Oyo town are fully aware of the dangers in online social networking, their actual practice of making themselves vulnerable contradicts this knowledge. This clearly shows the urgent need for serious media education. The dangers in SNS sites are real. With many victims already recorded in the country, the inability of the young adults to restrict the amount of personal information made available on SNS sites is worrisome. The lure of social media is so great and almost irresistible that students hardly think about the high premium of mindless exposure to online predators. This study recommends both preventive and corrective approaches to the problem. From the preventive angle, there is the need for serious media campaign aimed at sensitizing the young ones on the need to engage online protective measures. One of such measures is the use of privacy control to restrict the level of access to their personal information online if at all it is not possible to remove such information. The preventive measure is the introduction of media education in the National Curriculum right from secondary school. The inclusion of media education in the National Curriculum will definitely prepare young people for responsible and safe adoption of technological innovations and equip them with the knowledge of the dangers as well as protective measures that they can deploy to forestall all possible associated dangers.

References

- Boyd, D.M and Ellison, N.B (2007) Social network sites: Definition, history and scholarship. *Journal of Computer-mediated Communication*. 13(1) 210-230.
- Heverly, R.A (2008) Growing up digital control and the pieces of a digital life. *Digital youth: Innovation and the Unexpected*. 4: 199-218
- Pempek, T.A. Yermolayeva, Y.A and Calvert, S.L (2009) College Students' social networking experiences on Facebook. *Journal of Applied Developmental Psychology*, 30(3), 227-238.
- Natalie Gilliam (2011) The potential dangers of social networking: Teens an families need to be aware of negative effects. Retrieved from www.pearltrees.com on 2013/01/07/ doi: id5145657
- Tania Dworjan (2011) Problems for students using Facebook. Retrieved from www.socialnetworking/lovetoknow.com 2013/01/07/
- Jenney Cheever (2010) Five dangers of social networking sites. www.life123.com Retrieved:2013/01/07