South African Journal of Information Management
ISSN: (Online) 1560-683X, (Print) 2078-1865

An investigation into users' information security awareness on social networks in south western Nigeria

Authors:
Julius O. Okesola[1]
Adebukola Onashoga[2]
Afolakemi Ogunbanwo[3]

Affiliations:
[1]School of Computing, University of South Africa, South Africa

[2]Department of Computer Science, Federal University of Agriculture, Nigeria

[3]Department of Computer Science, Tai Solarin University of Education, Nigeria

Corresponding author:
Julius Okesola,
48948535@mylife.unisa.ac.za

Dates:
Received: 12 Nov. 2015
Accepted: 12 June 2016
Published: 21 Nov. 2016

How to cite this article:
Okesola, O., Onashoga, A. & Ogunbanwo, A., 2016, 'An investigation into users' information security awareness on social networks in south western Nigeria', *South African Journal of Information Management* 18(1), a721. http://dx.doi.org/10.4102/sajim.v18i1.721

Copyright:
© 2016. The Authors. Licensee: AOSIS. This work is licensed under the Creative Commons Attribution License.

Read online:
Scan this QR code with your smart phone or mobile device to read online.

Background: Social networks (SNs) offer new and exciting opportunities for interaction among people, cutting across different stratum of the society and providing a ubiquitous mechanism that supports a wide variety of activities. They are at the same time being exploited by criminals to fraudulently obtain information from unsuspecting users. Unfortunately, the seamless communication and semblance of safety assumed by most users make them oblivious to the potential online dangers.

Objective: Using quantitative methods on selected social sites, this study empirically examined the information security awareness of SN users in south western Nigeria.

Method: A self-designed research instrument was administered for data collection while descriptive and inferential statistics were employed using chi-square, cross-tabulation and *t*-test for data analysis and result interpretation.

Result: Findings from the analysed data suggest that the risk perception vary among male and female SN users and that the general perception of risks regarding SN usage is also very low.

Conclusion: Adequate security awareness coupled with detailed legal measures are required to keep SNs secured. However, an individual is duly responsible for the habit of ignoring potential risks posed by the networks.

Introduction

According to Terragon Ltd. (2013), Nigeria had the largest Internet population in Africa and was 11th in the world as of October 2013. Furthermore, social networking was the second-top (72%) activity on the net after 'news and information' (78%). As on June 30 2015, Nigeria had 15 million monthly active users, all of them using mobiles to like, share and upload content on the social network (Reuters 2015).

Social networks (SNs) or social media offer new and exciting opportunities to myriads of Internet users to communicate in real-time, explore business and entrepreneurship opportunities, socialise, promote different initiatives and obtain feedback for various activities. Although the positive role of SNs for various activities have continued to expand in recent times, sinister users and cybercriminals have also continued to explore them as a subtle means of attacking and exploiting unsuspecting and naive users. It is the observation of the authors that more users in Nigeria are migrating to Internet platforms on a daily basis as a way of identifying with the new age.

In the same vein, the Internet has also offered an online platform to conventional criminals (with the anonymity afforded by the Internet) who simply migrate online to have an extended reach of their nefarious activities beyond their immediate environment and to increase their pool of victims. Therefore, research is warranted into how social media can be kept safe from criminals *vis-à-vis* the extent to which users understand how much of the danger SNs pose in terms of awareness and mitigation.

SNs are functional platforms where Nigerian entrepreneurs can effectively communicate with Nigerian consumers to elicit useful information that will be of great benefit to the business (Angela 2011). Considering the level of usage of social media in Nigeria for other purposes, questions needs to be asked as to how these media have helped in raising awareness for locally made Nigerian products and/or services. On the other hand, researchers should also seek to know if users' awareness on social media has done more in promoting foreign brands at the expense of locally made goods among Nigerians.

This research is not particular about business opportunities, buying behaviour, products or services. However, it seeks to evaluate the impacts of information security awareness (ISA) on the use of social network sites (SNSs) using quantitative methods.

Social network sites and online activities

Social media are web-based applications that leverage Web 2.0 technology for the creation and exchange of user-generated content (Kaplan & Haenlein 2010). Generally speaking, they have become a significant technological phenomenon of this century with many of them being ranked as the most visited websites worldwide (Okesola 2015; Smith 2013).

Presently, there are numerous popular SNs, with Facebook, Twitter, LinkedIn, Myspace and Google+ being widely used worldwide (Smith 2013; Vaughan-Nichols 2013). Others include Sphere and Nexopia (Canada); Bebo, VKontakte and Hyves (The Netherlands); Draugiem.lv (Latvia), Ask-a-peer and StudiVZ (Germany); iWiW (Hungary); Tuenti (Spain); Nasza-Klasa (Poland); Tagged, XING, Badoo and Skyrock (parts of Europe); Orkut and Hi5 (South America and Central America); LAGbook (Africa), Mixi, Wretch, renren and Cyworld (Asia and the Pacific Islands); and Pinterest (India) among others (SNS 2014).

The increasing use of SNs and its popularity all over the world are evidenced by the number of users; social, economic and political initiatives; religions and businesses it now supports. Pressure groups are also supported and promote their ideology using SNs. The Arab spring demonstrations of 2010 and 2011 are a recent example of how SNs can be used to upturn governments and reshape political order. In south western Nigeria, more users are migrating into the SN environment with the associated advantage of visibility, connectivity and business opportunities offered by social media (Angela 2011; Evolution Africa 2012).

Social networks as people connector

Initially, SNs such as LinkedIn, originated from online communities that shaped around a common interest. These community sites include, but are not limited to, Reptile forums, photo, Wendy Johnson, thread of the day and Startrek (Saver 2009). Even though such sites are still in existence with anti-social common interest (Micheal 2010), SNs like Facebook have moved to congregate around groups of people instead. These sites are now characterised with a structure that clusters persons with similar and confined interests, which largely simplifies their communication with other members of their offline SNs (Boyd & Ellison 2007). In essence, physically dispersed users who were previously or presently friends or acquaintances in the offline mode can easily connect using computers and keep their interests or binding culture alive through social media. SNs also assist them through extrinsic affiliations with persons belonging to their friends' SNs (friend of a friend) to increase their pool of friends and social nets.

For example, Facebook recognises each member of an unlimited social community as a friend, despite the fact that most often, the social connection may be loosely acquainted with no form of intimacy (such as a friend of a friend). Among other usage, SNs such as MySpace and Facebook have become a primary meeting point for different categories of people aiming at socialising and exchanging ideas (Duven & Timm 2008). This connection is established by creating a profile that is comparable to a private home page (Boyd & Ellison 2007), which typically contains a selection of personally identifiable data, including contact information, name and demographic data. It is easy for users to post their videos and pictures, including their friends' videos and pictures, and subsequently tag them by name. Additionally, users' activity may be communicated to their online friends via the SN's news feed (Livingstone 2008). Hence, SNSs are achieving their original purpose to facilitate social interaction among individuals of similar choice.

Social networks as business enablers

Research has shown that users share opinions and make recommendations on SNSs (Tufekci 2008). On these sites, consumers seek others' opinions when considering the purchase of products and services. In fact, 78% of global consumers say they trust and believe other people's recommendations for products and services more than any other medium (SNS 2007). Social media are now being used to create economic dynamics and the marketing mix required to nurture and grow indigenous business enterprises and promote social interaction among a growing population of users.

Members of SNSs serve two roles; they both supply and consume content. The creators of content are typically highly engaged consumers and, as a result, influential. If the proper influencers are reached with a message that they perceive as valuable, it can create a chain reaction for promoting goods and services among consumers. This is tremendously powerful to marketers because in these scenarios, users subtly accept such information in passing as very active introduction to products or services. Users on SN also provide information on their profile while joining such sites.

This information is invaluable to marketers as they can be used to develop highly targeted marketing adverts to reach potential consumers (Esma, Sebasten & Ho 2010). Facebook emerged on the SN scene over half a decade ago; originally viewed as a networking site limited to college students. In 2006, Facebook was serving as many as 7.5 million registered users and was ranked seventh among the more accessed websites in the United States (Budden & Budden 2009; Colleen 2009; Gaudin 2002).

Recruiters for businesses and colleges are looking for the social and professional networks to perform background checks on potential employees. In the past, many companies used Google and Yahoo to perform these background checks, but recently, Facebook, MySpace, Xanga and Friendster are being used in this regard (SNS 2007).

Vulnerability to attacks

While the majority of website users do not pose a threat, malicious individuals might be drawn to them because of the ease of access to data and the volume of available personal information (Saldarini & DeRobertics 2003; Tony 2009). This information could eventually be used to launch social engineering attacks. Social engineering involves luring unsuspected users to take cyber bait in much the same way that conventional fishing involves luring a fish using bait (Livingstone 2008). Phishing is a form of social engineering that deceives consumers into disclosing their personal and financial data, such as passwords, ATM pin numbers, credit card numbers and bank account numbers. It is an attempt to elicit a specific response to a social situation that the perpetrator has engineered (Granger 2006; Tufekci 2008). Phishing and identity theft scams are on the increase in Nigeria among other forms of cybercrime (Longe & Osofisan 2011).

Information security awareness on social networks

SNs are continuously changing and influencing the way individuals communicate by offering real-time and exciting opportunities for interaction among people; cutting across different stratum of the society and providing a ubiquitous mechanism that supports a wide variety of activities. Unfortunately, the seamless communication and semblance of safety assumed by most users make them oblivious to the potential dangers to which they are exposed online.

In the same vein, social media are being exploited by criminals who are aided by the anonymity in cyberspace. Cybercriminals are exploiting user ignorance and their level of awareness of the dangers lurking in cyberspace to victimise users thus making them vulnerable to different forms of attacks such as spamming, phishing, advance fee fraud and all other sorts of online fraud while online.

To mitigate this risk, many SN providers have started incorporating awareness programmes for their self-protection as well as their services (Okesola 2015). This study investigates the level of user's awareness of security vulnerabilities in online communities in south western Nigeria. It aims to assess the perception of online risks among users as well as the level of awareness of risks posed to online SN users.

Related works

SNSs have come along with many opportunities as well as challenges for communication. Google is the most visited website in the world (Wikipedia 2012; Shamim 2011); however, it has been competing favourably with Facebook. As of September 2011, Facebook was already hosting nearly a billion users (Judge 2011; Zonealarm 2010) and is ranked as the world's largest SN (Kyle 2011). A survey carried out between February and June 2011 presented Facebook as the second most visited site in the average country in the world (Wikipedia 2012), with specific statistics also confirming its second place position in both the United States and the United Kingdom (Shamim 2011).

The privacy risks are more noticeable nowadays in SNSs than other sites and blogs, as SNSs offer a sense of intimacy to online friends and acquaintances (Facebook Inc. 2012). Besides, due to the motivation offered by SNSs to communicate and maintain relationships, the quantity of data divulged by the users are much greater when compared with other media. There exist fake dating sites, phishing websites that steal personal details and other forms of vices to lure unsuspecting users into divulging personal information.

This section looks at related research that has been done on ISA and SNs. In particular, research done on the effect of anonymity and SNs, social engineering and SNs' impact on personal information gathering is investigated.

Anonymity on social networks

Anonymity has been an aid to many crimes perpetrated on the Internet (Longe & Osofisan 2011). Although anonymity is characterised as the essence of users' privacy, the perceptions of anonymity online provides a means for invasion of privacy and creates a platform through which various vices using social engineering (the act of fraudulently obtaining information from unsuspecting users) can be accommodated on SNs (Redbridge Marketing 2012; Tufekci 2008).

As SNs continue to expand and advance, social interaction as the primary vehicle through which advancement of information and communications technology affects socio-economic outcomes has remained one of the most popular ways of exchanging information and promoting ideas. This trend has led to an increase in the adoption and use of SNs as a means of interaction between users. However, the alleged anonymity of online relationships weakens the sense of responsibility experienced when communication takes place in person (Olaoti 2011). For example, it is the authors' observation that computer users are more comfortable to divulge personal information in an online narrative on a faceless SN page, than confiding personal information to somebody sitting in front of them. People tend to be cautious in providing personal information when asked for it by strangers, yet are comfortable to provide their personal details on their SN home page. The weakened sense of responsibility relates to the person divulging personal information on the Internet, accessible to anybody with the technical know-how to retrieve the data.

Social engineering

Social engineering uses subtle persuasions to influence unsuspecting Internet users and social media subscribers into divulging confidential information and performing actions that they would ordinarily not do. While closely related to simple fraud or a confidence trick, the term applies to how computer criminals and cybercriminals trick their victims to gather information. In most online cases, the attacker is not in any physical contact with the victims, and information can be obtained from the victim via social media or other websites (Budden & Budden 2009; Rusch 1999; Wild Fusion 2010).

In Nigeria, fake recruiters for employment now use SNs to lure job seekers into filling fake employment forms and paying money to seek employment in non-existent organisations (Olaoti 2011). The intending applicants are then invited to take employment tests or interviews after which the fake recruiters disappear into thin air.

Although SNSs have varying features, they all permit individuals to supply information about themselves and subsequently provide some communication mechanism (such as forums, e-mail, chat rooms and instant messenger) that facilitate the connection of users to other users (Duven & Timm 2008; Tufekci 2008). It is now possible on some SNSs (such as Twitter and Facebook) to become friends with other users using shared connections. Social engineering sites depend strongly on Internet communications and connections to encourage individuals to supply a certain amount of private information. When deciding the volume of data to reveal, users generally do not exercise enough caution as they would ordinarily have when meeting someone in person. This could be traced to the fact that the Internet presents a feel of anonymity and that the dearth of physical relations bestows a false sense of security.

Consequently, these data fraudulently obtained could be employed to conduct social engineering attacks. For example, most social sites have subgroups or communities of a particular interest. However, the social sites, while creating some potential advantages for business organisations to market and promote business activities and interact with customers by requesting for intending customers to supply personal details presents security challenges that have become a major area of concern as personal information can also be used by criminals.

One major area of concern is the use of cyber baits by criminals just like in conventional fishing that requires luring a fish using bait. Victims are tactically deceived into divulging their private and financial data, such as ATM pin numbers, bank account numbers, passwords and credit card numbers. It is also a calculated attempt to draw out a particular response to a social situation engineered by the perpetrator (Tufekci 2008). Phishing scams seem to be the highest on the increase among all other forms of cybercrime worldwide and in Nigeria in particular (Olaoti 2011). This is evidenced by data from Kaspersky Lab as far back as 2009 where over 43% of SNs' users have already experienced phishing attacks in one way or the other (Wild Fusion 2010).

Research methodology

The study conducted for this research paper uses quantitative methods on selected social sites to examine the ISA of SNs' users in south western Nigeria. This section addresses the research methodology followed for the study.

Research design

The research sets out to investigate users' ISA on SNs in south western Nigeria. A self-designed research instrument titled 'Information Security Awareness on SNs' constitutes a tool for gathering data across different strata of Internet users for the research. This study is limited to Internet users in south western Nigeria covering the major capital city for each state, viz, Lagos, Akure, Ibadan, Abeokuta, Oshogbo, Ilorin and Ado-Ekiti.

Study sample

The research sample consists of various categories of social media users ranging from students, workers, youths (employed and unemployed) to working class adults. Questionnaires were distributed by hand and through e-mails to users based on their understanding of the research objectives and their familiarity and use of the social media platform. A total of 293 questionnaires were distributed out of which 247 were selected for satisfying stratification for age, gender, educational level and length of usage of Internet.

Sampling technique

The sampling technique used in this research work is the stratified sampling method in combination with simple random sampling. The simple random sampling technique is a method employed in selecting a sample of considerate size from a given population of data used in the survey. The estimate from the population in simple random sampling to get the sample size from the given population is one in which every response has the same probability of being chosen.

Research instruments

A self-constructed questionnaire titled 'Librarians' Attitudes to Computerized Information Systems (LACIS)' was the main instrument used to collect data for this study. The questionnaire used contains 30 items grouped into three sections. Section A requests for the background information of the respondents while section B elicits information on the respondents' work experience and knowledge of computer usage. Section C only measured attitudes of respondents towards computerised information systems. The librarians responded on four likely points: strongly agree, agree, disagree and strongly disagree.

Validation of the Instrument

The face-validity and content-validity of the instrument were verified by experts in the University of Ibadan. Various suggestions made were used to modify the instrument.

Reliability of the Instrument

In order to ascertain the consistency of the instrument, a test–retest method was used to ascertain the reliability of the instrument. The questionnaire was administered twice to a group of five professional librarians randomly selected from the sample of the study. The interval between the first and second administration was 2 weeks. A correlation coefficient of 0.86 was achieved, which was considered high enough to justify the reliability of the questionnaire.

Administration of instrument

Since the Nigeria SN population stands at 15 million as at June 2015 (Reuters 2015), a sample size of 3 million was considered statistically significant for the study.

Valid e-mail addresses of social media users were therefore obtained from bulk Short Message Services Vendors, conference mailing lists, seminars and workshops to obtain the list of respondents. The research instrument was administered by hand and through the e-mail addresses of the recipients in south west Nigeria and a group of research assistants from the University of Ibadan, Department of Computer Sciences followed up with the instrument.

Formulation of hypothesis

To guide the research and data analysis for the categories, the following hypotheses were formulated:

$\mathbf{H_{1o}}$: There is no significant relationship between male and female users in respect of their awareness of potential online risks when using social media.

$\mathbf{H_{2o}}$: There is no significant relationship between users' awareness of potential risk online and the use of SNs for interaction by the generality of users.

Data presentation and analysis

What follows is a summary of data gathered from the respondents. Table 1 shows the frequency of responses from male and female users. Table 2 reflects the academic or educational levels of the respondents. While Table 1 shows that there are more male social media users than female users in the study sample, Table 2 shows that SN usage is more prevalent among tertiary-level users in the study sample.

Table 1 present three percentage columns. The *percent* column reflects the number of respondents as a percentage of all participants, including the people who did not answer. The *valid percent* column expresses the number responding as a percentage of those who responded. In this scenario, *valid* simply means that a respondent answered the question; it is not an endorsement of its psychometric validity. The *cumulative percent* column adds up the preceding percentages to arrive at a 100 percentage total.

Table 2 provides the descriptive statistics for educational level of SN users. It is indicated from the statistics that users with tertiary-level education are more than all other categories of users (57.5%) while secondary school–level education users are just 4.5%. This demography is indicative of the most active users among the study population.

In Table 3, the results of the *t*-test statistics carried out on the means scores in respect of hypothesis 1 indicated that there was significant difference between the mean value of responses of the female and male respondents. The male values are 10.77 and 20.68, respectively, for the different classes of respondents while those of female respondents are 5.7 and 18.7. A negative mean difference between the sampled and hypothesised population is usually indicative of insignificant difference. However, a positive mean difference of 10.77 – 5.7 = 5.07 for the female users and 20.68 – 18.7 = 1.98 for the male users reflects that there is a significant difference between the two sets of users, the male users lesser than female users. Hence, hypothesis 1 is rejected. This suggests

TABLE 1: The statistics on gender: Male versus female respondents.

Gender	Frequency	%	Valid Percent	Cumulative %
Male	148	59.9	59.9	59.9
Female	99	40.1	40.1	100.0
Total	**247**	**100.0**	**100.0**	-

TABLE 2: The statistics on respondents' educational level.

Institutions	Frequency	%	Valid %	Cumulative %
Secondary	11	4.5	4.5	4.5
Tertiary	142	57.5	57.5	61.9
Post-tertiary	94	38.1	38.1	100.0
Total	**247**	**100.0**	**100.0**	-

TABLE 3: Comparison of the female and male mean responses for analysis.

Gender	*N*	*X*	SD	*df*	*t*-cal	*t*-tab	*N*	*X*	SD	*t*-cal	*t*-tab	*df*
Female	100	6.7	5.7	29	2.69	-	100	18.7	6.3	3.0	2.18	-
Male	100	10.77	3.4	-	-	2.04	100	20.68	3.5	-	-	28

$p < 0.05$ level.

NS, not significant; *N*, total number; *X*, mean; SD, standard deviation; *df*, degree of freedom; *t*-cal, calculated *t*-test; *t*-tab, tabulated *t*-test.

TABLE 4: Comparison of general mean responses for the population.

Variables	Mean	SD	*N*	*df*	*t*-cal	*t*-critical
Positive response	14.57	3.6	30	58	10.0*	2.04
Negative responses	23.6	3.2	30	-	-	-

*, Significant at $p < 0.05$.

N, total number; SD, standard deviation; *df*, degree of freedom; *t*-cal, calculated *t*-test.

that male users are more conscious of security vulnerabilities on SNs than female users and that gender has a significant influence on risk awareness in social media usage.

In Table 4, the mean scores of combined responses for the *t*-test statistics carried out on these mean scores indicated a *t*-test result of 2.04 at $p < 0.05$. The mean scores for both groups are 14.57 and 23.6, respectively. The mean score of respondents who are negative about ISA (23.6) is higher than that of the mean score for the positive respondents (14.57), a difference of 9.03 for the combined responses. This analysis is predictive of the fact that more SN users lack the awareness of the security vulnerabilities to which they are exposed on SNs. A *t*-test result of 2.39 is very significant. Hence, null hypothesis is rejected, implying that users are generally not aware of the online risk portended by social media usage.

Discussion

This research study employed quantitative methods to evaluate the level of awareness of security risks to which users of SNs are susceptible in south west Nigeria.

Discussions of oral responses

A sizeable percentage of respondents revert to the fact that although SNs are supposed to provide some level of assurances through the certainty of established relationships with contacts, infiltrators are capitalising on the ability to take up personalities on SNs as a way of perpetrating fraudulent activities. Oral responses also revealed that most users are oblivious of security vulnerabilities and simply enjoy the seamless platform offered by SNs for interaction, marketing, publicity and in some cases education. However, online dating using SNs flags 'very red' among respondents. Most of them shy away for overtures for dating and any form of emotional involvements with unknown personalities.

Discussions of responses from questionnaire

Findings from the data analysed suggest that the perception of risk vary among female and male users with the male users being more conscious of risks than the female users. The analysis also supports the fact that although some categories of users exercise some caution on SNs, the majority of the users polled are oblivious to the risks on SNs, indicating that their level of awareness is low. The extent to which users are aware of these risks was in this discourse and findings from data analysis indicated that the perception of risks does not vary among female and male users of SNs. Users see anonymity as the main impetus that fuels crime on social media.

Implications for research and practice

Findings from this research support the fact that SN awareness for different forms of interaction and communication is on the increase in Nigeria. In the same vein, a number of users have fallen victim to the activities of nefarious users who have simply turned SNs into a tool for criminal activities such as phishing, scamming and other forms of vices that occur daily on SNs. Therefore, it has become imperative that research be undertaken to further come up with frameworks that can be employed to educate users on the volume and type of risks that SN portends in order to guarantee healthy and constructive usage and empower users as the last line of defence in the quest to make SNs safe and secure. Practically, users of SNs must understand the dangers posed by connecting to individuals with whom they have no prior relationship in the offline mode. Product and/or services marketing on SN platforms must be subscribed with caution and double checked for authenticity.

Contributions to the body of knowledge

This study contributes to the body of knowledge on SNs by providing insights into present trends in the diffusion, adoption and usage of social media for online interactions in Nigeria. The analysis of the data collected revealed that sex and experience have a significant influence on users' attitudes and perception of risks on SNs. This study also contributes to the theoretical findings by providing baseline data on the attitudes of users of SNs in Nigeria.

Conclusion

Keeping SNSs safe will definitely involve a combination of educative, technological and legal measures, but ignoring the risks posed by these networks is at the individual's peril.

Acknowledgements

Competing interests

The authors declare that they have no financial or personal relationships which may have inappropriately influenced them in writing this article.

Authors' contributions

O.O. was the project leader, who wrote the manuscript and performed most of the programme design and implementation. A.O. monitored the project and administered the research instrument including the questionnaire for the collection of primary data. A.O. was the project moderator and the reviewer of the programme, processes and research output.

References

Angela, H., 2011, *Social media marketing: Nigerian business presentation*, viewed 21 November 2012, from http://www.slideshare.net/angelahausman/social-media-marketing-nigerian-business-presentation

Boyd, D. & Ellison, N., 2007, 'Social network sites: Definition, history, and scholarship', *Journal of Computer-Mediated Communication* 13(1), 1–11, viewed 23 August 2012, from http://onlinelibrary.wiley.com/doi/10.1111/j.1083-6101.2007.00393.x/pdf

Budden, C. & Budden, M., 2009, 'The social network generation and implications for human resource managers', *Business and Economics Research* 7(1), 10–12.

Colleen, R., 2009, 'Safeguarding against social engineering', *Infosec Writers Library*, viewed 7 November 2012, from http://itmanagement.earthweb.com/secu/article.php/1040881

Duven, C. & Timm, D., 2008, 'Privacy and social networking sites: New directions for student services', 124, 89–100. http://dx.doi.org/10.1002/ss.297

Esma, A., Sebasten, G. & Ho, A., 2010, *Towards a privacy-enhanced social networking site. 2010 International Conference on Availability, Reliability and Security*, viewed 07 June 2011, from http://www.mendeley.com/research/towards-privacyenhanced-social-networking-site-17/

Evolution Africa, 2012, *The potential for social media marketing in Nigeria*, viewed 15 January 2013, from http://evolutionafrica.com/blog/

Facebook Inc., 2012, 'Latest development – Facebook', *The New York Times, Business Day*, 29 September, viewed 29 September 2012, from http://topics.nytimes.com/top/news/business/companies/facebook_Inc/Index.html

Gaudin, S., 2002, *Social engineering: The human side of hacking*, viewed 14 June 2012, from http://itmanagement.earthweb.com/secu/article.php/1040881

Granger, S., 2006, *Social engineering reloaded*, Security Focus, viewed 05 December 2012, from http://securityfocus.com/print/infocus/1860

Judge, P., 2011, '2011 social networking security and privacy study', *Barracusalabs Networks Inc*, viewed 03 February 2013, from http://www.barracudalabs.com/snsreport/2011socialnetworkingstudy.pdf

Kaplan, A.M. & Haenlein, M., 2010, 'Users of the world, unite! The challenges and opportunities of social media', *Business Horizons* 53(1), 61.

Kyle, A.H., 2011, 'Top 10 most visited website of 2011', *Kaleazy Creative*, viewed 23 July 2011, from http://Kaleazy.com/top-10-most-visited-websites-of-2011

Livingstone, S., 2008, 'Taking risky opportunities in youthful content creation: Teenagers' use of social networking sites for intimacy, privacy and self expression', *New Media Society* 10, 393–411, http://dx.doi.org/10.1177/1461444808089415

Longe, O.B. & Osofisan, O.A., 2011, 'On the origins of advance fee fraud electronic mails: A technical investigation using Internet protocol address tracers', *The African Journal of Information Systems* 3(1), viewed 10 January 2012, from http://digitalcommons.kennesaw.edu/ajis/vol3/iss1/2

Micheal, W., 2010, 'Community Vs. social network', *Lithospher*, viewed 19 May 2013, from https://lithosphere.lithium.com/t5/science-of-social-blog/Community-vs-Social-Network/ba-p/5283

Okesola, J.O., 2015, 'Measuring information security awareness effectiveness in social networking sites – A non-incident statistics approach', PhD thesis, School of Computing, University of South Africa (UNISA).

Olaoti, Y., 2011, *The branding gavel – Social media and Nigeria's market/brands*, viewed 27 December 2012, from http://yinkaolaito.com/2010/05/social-media-and-the-nigerias-marketbrands/

Redbridge Marketing, 2012, *Social network marketing: The basics*, viewed 04 January 2012, from http://www.labroots.com/Social_Networking_the_Basics.pdf

Reuters, 2015, 'Social media giant rakes in users in Nigeria and Kenya, eyes rest of Africa', *Pulse News Agency International by Reuters*, viewed 24 March 2016, from http://pulse.ng/tech/facebook-social-media-giant-rakes-in-users-in-nigeria-and-kenya-eyes-rest-of-africa-id4156292.html

Rusch, J., 1999, *The 'social engineering' of Internet fraud. INET '99 proceedings*, viewed 30 August 2012, from http://www.isoc.org/inet99/proceedings/3g/3g_2.htm

Saldarini, R.A. & DeRobertics, E.M., 2003, 'The impact of technology induced anonymity on communication and ethics: New challenges for IT pedagogy', *Journal of Information Technology Impact* 3(3), 121–130.

Saver, K., 2009, 'What is the difference between social networking and online communitiess?', *Cisco Support Community*, viewed 21 November 2013, from https://supportforums.cisco.com/thread/2103436

Shamim, S., 2011, 'Top 10 most visited websites in the world', *Expert Review now*, viewed 25 July 2011, from http://www.expertreviewnow.com/2011/02/top-10-most-visited-websites-in-the-world/

Smith, C., 2013, 'The planet's 24 largest social media sites, and where their next wave of growth will come from', *Business Insider*, viewed 09 December 2013, from http://www.businessinsider.com/a-global-social-media-census-2013-10

SNS, 2007, *Social network sites – Venues for the brand ambassadors of the future?* viewed 15 January 2013, from http://www.iprospect.com/media/article_sc_05_18_07.htm

SNS, 2014, 'Social networking service', *Wikipedia*, viewed 23 September 2012, from http://en.wikipedia.org/wiki/social_network_service

Terragon Ltd, 2013, 'State of digital media in Nigeria', *Terragon Insights*, viewed 22 March 2016, from http://twinpinenetwork.com/publications/Nigeria-%20State%20of%20Digital%20Media.pdf

Tony, B., 2009, *Gone phishing*, viewed 23 July 2012, from http://netsecurity.about.com/od/secureyouremail/a/aa061404.htm

Tufekci, Z., 2008, 'Grooming, Gossip, Facebook and Myspace: What can we learn from those who won't assimilate?', *Information, Communication, and Society* 11, 544–563, viewed 30 August 2012, from http://semuwemba.files.wordpress.com/2010/03/grooming-gossip-facebook-and-myspace.pdf

Vaughan-Nichols, S.J., 2013, 'Facebook remains top SN, Google+', *YouTube Battle for Second. ZDNet*, viewed 09 July 2013, from http://www.zdnet.com/facebook-remains-top-social-network-google-youtube-battle-for-second-7000015303/

Wikipedia, 2012, *Facebook. Wikipedia, the free encyclopedia*, viewed 01 November 2012, from http://en.wikipedia.org/wiki/facebook

Wild Fusion, 2010, *Social network marketing in Nigeria*, viewed 05 March 2013, from http://wildfusion.blogspot.com/2010/02/social-network-marketing-in-nigeria.html

Zonealarm, 2010, 'The dark side of social media: How phishing hooks users', *Zonealarm by Checkpoint*, viewed 21 December 2012, from http://www.zonealarm.com/blog/index.php/2011/07/how-phishing-hooks-users