THE INTERNATIONAL JOURNAL OF HUMANITIES & SOCIAL STUDIES

Smart Phone and Social Media Security and Privacy Management by Students of National Polytechnic University Institute, Bamenda, Cameroon

Njodzefe Nestor
Lecturer, School of Journalism and Media,
National Polytechnic University Institute, Cameroon
Fobang Geraldine
Postgraduate Student, Department of Peace Journalism,
Protestant University of Central Africa, Cameroon

Abstract:
This study investigates the major security and privacy challenges that social media and smart phone users experience and how they manage these security and privacy concerns. The worrying phenomenon of cyber criminality and personal security online is a major threat globally and with the growing numbers of smartphone users and internet dependency in Cameroon especially amongst students, people are susceptible to having their private information misused. The study addresses this threat by finding out the extent to which smartphone users in Cameroon are aware of security threats lurking online. The researcher employed a survey where questionnaires were used to collect data. The sample population was 100 respondents from the National Polytechnic University Institute, Bamenda, aged between 18-35 years who have access to smartphones and are active social media users. Findings reveal that most people are aware of some of the threats to privacy on social media and smart phones. However, it was evident that some respondents do not safeguard their privacy when accessing social media sites.

Keywords*: Social networks, smartphones, security, privacy*

1. Introduction

Social Networking websites such as Facebook, Twitter, WhatsApp and MySpace have been growing rapidly within the past few years with now over two billion users. Virtually every computer literate individual has at least one social network account, and they spend most of their time on social networks each day.

Social networks can be described as web applications that allow users to create their semi-public profile (Boyd, D.M, 2007) i.e. a profile that some information is public and some is private, communicate with those who are their connections (friends), and build an online community. It is based on social relationships among users. A majority of people subscribe to social networks to share or get information and also to keep in contact with their friends.

Social networks and smart phones have opened up a new avenue of communication for millions of people around the world. The major attraction of these technologies is the ease with which people can share their personal information with their friends. What makes smartphones peculiar is that they have features of both a mobile phone and a computer, allowing people to talk, text, access personal and work e-mail, browse the Internet, make purchases, manage bank accounts, and take pictures. (Scott, M. 2016)

The uptake of social media and smart phones and or similar devices is at an all-time high in Cameroon just like in other African Countries.

There has been a significant evolution in the access to Internet by Cameroonians with a growing Internet penetration rate averaging 14% per year between 2007 and 2011 and 19% between 2012 and 2017 below the 32% of continent-wide penetration (Alliance for Affordable 22 Internet -A4AI 2014, Doing Business in Cameroon 2017, Global Internet Open Information 2017).

Internet Live Stats indicates that 4.3 million Cameroonians which was approximately 20% of the population had access to the Internet in 2016. During this same period, a report on mobility published by the management of the Cameroonian subsidiary of the Swedish telecoms firm Ericsson in December 2016, indicated that access rate in Cameroon reached 25.6% as at the end of December 2015. These figures reveal that Internet access in Cameroon is higher compared to its counterparts in the sub-Saharan African region, which was at only 20% over the same period. Between 2006 and 2016, the Internet bandwidth has significantly increased, moving from 159 to 32 500 Mbits for international band and 132 to 40 000 Mbits for national band.

Generally, in Cameroon like its counterparts in sub-Saharan Africa, mobile telephony has grown much faster than Internet usage. ITU puts Cameroon's mobile penetration rate at 61 percent with 17% the mobile users estimated to own mobile phones (M&C Saatchi Mobile 2013). This correlates with Cameroon's Telecommunication Regulatory Board 2016

Annual Observatory which indicates that 40% of the 18 million mobile phone operators were connected to the Internet via phone as more subscribers had smartphones. The report further states that subscription to the Internet from the operators of fixed networks witnessed a sharp rise of 167.08% in 2016.

With this rise in mobile penetration and data access, comes a corresponding rise in social media and smartphone use in the country. The uptake in smartphone use in the country has sparked a debate on issues surrounding privacy, largely because the number of personal information new media users freely share on social media and smartphone platforms is astounding. Ekoa Regina M.M (2018), observed that the high use of smartphones has shifted cyber threats from desktop computers to these new devices.

According to Norton cybercrime report, 978 million people in 20 countries were affected by cybercrime in 2017. Mobile vulnerabilities have grown as people use their gadgets online more frequently.Cameroon's National Information and Communication Technologies Agency (ANTIC) in 2017 audited 74 public and private organisations on their exposure to cyber-criminality and 8,954 weaknesses were detected.

In 2015, the mobile phone sector in Cameroon lamented losses of FCfa 18 billion for operators; another FCfa 4 billion for the State. According to the 2014 report from the National Anti-Corruption Commission, cyber-criminality cost FCfa 3.5 billion to Cameroon between November and December 2013.

The fact that the Government has done little to address the issue of cybercrime and personal security online coupled with the growing numbers of smartphone use and internet dependency means that Cameroonians online are susceptible to having their private information misused.

To this end, this study will seek to find out the extent to which student smartphone users in Cameroon particularly those of National Polytechnic University Institute are aware of security threats lurking online. It will also attempt to identify the measures employed to safeguard their privacy on social media and smartphones and how effective these measures are.

1.1. Research Objectives

This study is guided by three objectives which are: -

- To establish the level of awareness on privacy and security threats among social media and smartphones users.
- To identify the privacy and security challenges that Smartphoneand social media users on are experiencing.
- To determine the extent to which privacy and security concerns have influenced online behavior of smartphone users.

1.2. Research Questions

- Are respondents aware of any threats to privacy on social media and smart phones?
- Is the online behavior of the respondents shaped by privacy or security concerns?
- Which measures have respondents taken to protect their privacy on smartphones and social media?

2. Related Literature

2.1. Security and Privacy in Social Networks and Mobile Apps

Information in social networks are 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 (Gross, R. and Acquisti, A. 2005). 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 (Tuunainen, E. and Pitkänen, O. 2009)

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, (Strater. K, Richter, H. 2011) examined privacy and disclosure of information in a social networking community while (Zhou, B. and Pei, J. 2008) 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 (Korolova, L. et al 2008).

Luo, W ET all 2015 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 by Goettke, R. and Christiana, J. (2007), while Gross, R. and Acquisti, A. (2005) researched on user's awareness of privacy on online social networking sites. Further, Gummadi, K., Krishnamurthy, B., & Mislove, A. (2013) 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 (Harris, R.D 2013). 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 (Lipford, H. R., Besmer, A. & Watson, J. 2009).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 applications that does not require internet connection to access them, the likelihood of students to use them for learning is high.

Zheleva, E. M., Terzi, E., & Getoor, L. (2012) asserts that the 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.

2.2. Theoretical Foundation

The theoretical foundation of this study is on the principles of Communication Privacy Management Theory. The theory explains the self-disclosure procedures both online as well as on social states. It aims to define how a disclosing persons and recipient handle their privacy boundaries and disclose confidential information. Having a social media profile often puts the users in constant conflict between wanting to share and keeping information private. By virtue of having a profile on social media, users mean to share their lives with their friends, followers and sometimes the general public , they do so via status updates, photos, videos, vines, tweets and events: there is a conflict arising because they want to share the information but some opposing need for privacy still exists. Petronio argues that information starts out as private with thick boundaries but when sharing of this information is done on social networks or on smart phone apps the boundaries become thinner and more porous as more people get access and rights to re-share the same information. This theory ties in with this study as it examines the process by which all information transitions from privately owned and how the boundaries can progressively thin until information becomes public. We farther examine how boundary turbulence occurs because the friends we share information with on Social networks and using smartphones are usually not in close proximity and there is rarely any opportunity to agree on privacy boundaries and rules surrounding re-sharing.

3. Research Methodology

This study primarily utilized survey which was conducted through the administration of questionnaires. The study was conducted at National Polytechnic University Institute Bamenda, Cameroon due to the abundance of a smartphone and social media users. The target populations of this research were the youths in the University, aged between 18-35 years. The stratified random sample was used to ensure an equal representation of students across all disciplines offered in the University. The sample size chosen was 100 questionnaire respondents. The collection of primary data was done through questionnaires which were administered through research assistants in the different schools. The questionnaires had a balance of carefully constructed closed and open-ended questions, which facilitated the collection of both qualitative and quantitative data.

4. Findings and Discussions

This section provides findings of the study. A total of 100 students participated in the study. Findings of the study are presented based on identified themes as follows.

4.1. Social Networking Habits and Patterns of the Respondents

As regards the number of respondents on the various SNS, all the respondents acclaimed to belong to at least one social media site with three quarters of them being on at least 5 social networking platforms with the most popular being: Whats App, Facebook, Twitter, YouTube, Google+ and LinkedIn. These findings clearly show that a majority of SNS users use multiple platforms online. The respondents were also profiled on the basis of preferred devices on SN access and uploading content. It was found that 75% of the respondents preferred to access the Social Networks on smart phones while 60% used the same smartphones to primarily share content such as photos and videos on social media.

4.2. How Reasons Respondents Choose Their Devices

The respondents were asked for the exact reasons they chose the device they preferred. It was found that 40% of them chose their preferred device because it was the most convenient, 30 % agreed it was due to ease of accessibility to them while 12% said they chose their device because it was users friendly and 18% gave other reasons such as: large screen, the device was very secure, the content was already on the device and that the device that allowed them more editing options/features for their content.

These findings imply that social media access is done spontaneously as an overwhelming majority (over 92%) gave reasons for choosing their devices as availability, accessibility and convenience. This is probably why only 7% of the respondents will use a desktop computer as it is not a device you have on the go. The reasons the sharing of content was slightly higher on computers were ease of editing and more stable internet access for heavier files. The implication is that fixed data is still more reliable for larger content sharing tasks that mobile networks. It also implies that most people will alter. Edit and manipulate the information they post and need more computing abilities for this.

4.3. Time Spent Online and on Social Media Sites

As regards the time spent online and on social media sites, 32% of the 100 respondents said that they spent at least 4 hours online every day but only 18% spend under an hour on social media sites per day. This means that more than half the respondents were online daily. Only about a quarter of the respondents said their access varied from day to day, while three quarters were online daily. The implication is that there is potential to disclose some information about your life, activities, likes, location and opinions multiple times a week and there ought to be a corresponding urge to learn about how that information is shared, viewed or sold. In comparison less than 5% of the respondents were on social media daily but a majority logged on to some social media platform every week.

4.4. How Respondents Use Their Social Media Account

The respondents said they used social media for a variety of reasons including: - keeping up with friends that they actually know well in person, staying connected with people with interests similar to theirs (known and unknown), staying in touch with family and friends who are not always nearby, share and follow issues of social-political significance, conducting business online, sharing content that they created and to keep up with trends.

4.5. Awareness of Threats to Privacy on Social Media and Smart Phones

When questioned about their concern on internet security, 80% were very concerned, 14% expressed some concern in varying degrees. The only respondents who admitted to not being concerned at all constituted 5%. At least 71% or over two thirds of the respondents were aware of the following threats to online privacy and security: -Identity theft, phishing, smartphone sharing/tracking their online habits and banking fraud. In a seeming contradiction to the responses above, when respondents were asked what was more important between privacy and convenience, majority said privacy. At least 82% of the questionnaire respondents admitted that they were very concerned about security on the internet in general. Over three quarters % of all respondents knew of the following threats to online privacy and security: unauthorized access to their accounts by 3rd parties, phishing, smartphones keeping track and sharing their profiling data with other apps as well as profiles being cloned.

4.6. Behaviour of Respondents to Safeguard Their Security Online

Respondents were asked how they would respond to their social media accounts being breached/hacked or compromised and 55% said suggested they will change the password while 27% said they will deactivate the account and 9% said they will contact and inform service provider as a similar 9% posited that they all inform all their friends on site to create awareness. Similarly, 43% of the respondents said that if their handsets were breached/ hacked or compromised, they would change passwords and 41% wipe device memory. On both social networks and smartphones, the most popular reaction was to change passwords. There were several things that respondents said they did to protect their privacy. 65% said that they only followed or accepted friend requests from people they personally knew well. Another 35% never post personal photos and their locations on social media. These findings show that security measures among social media and smart phone users are still lax in comparison to how much they know about the threats to their privacy. The reasons could be carelessness, not knowing the real-life impact of these threats as well as trivializing online threats as minor with no actual losses incurred from them.

5. Conclusion

The study aimed at assessing student's awareness of security and privacy when using social networks and mobile devices. In particular, the study investigated NPUI 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 NPUI and by extension other higher learning institutions in Cameroon lack basic skills and knowledge on using social networks and mobile devices and therefore not ready to engage themselves in using social networks and mobile devices. 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 to adopt social networks. In addition to that, loss of privacy may cause economic losses and destruction of social image of individuals in the society. Furthermore, loss of privacy may jeopardize physical security of social networking users as well. It was therefore recommended that industry players in smart phones and Social networking in Cameroon should work to raise awareness for users and to simplify terms and condition. The law enforcement agencies in the country should also be more open to following up cybercrimes and treating cybercrime just as seriously as they do other crimes. If citizens were to see these issues as real crimes, they might take the threats more seriously.

6. References

i. Bikoro, D.F, Samuel, J. R, Kala, K. (2018). Determinants of Cyber Security Use and Behavioral Intention: Case of the Cameroonian Public Administration. 10.1007/978-3-319-77712-2_104.
ii. Boyd, D.M and Ellison, N.B (2007) "Social Network Sites: Definition, History, and Scholarship," J. Computer-Mediated Communication, vol. 13, no. 1, pp. 210–30. http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html

iii. Ebongue, J. L., (2015). Rethinking Network Connectivity in Rural Communities in Cameroon, University of Ngaoundéré, Ngaoundéré, Cameroon
iv. Ekoa Regina, M.M (2018), "A review of Cybercrime in Sub-Saharan Africa: A Study Cameroon and Nigeria", International Journal of Scientific & Engineering Research Volume 9, Issue 5, May-2018 211, SSN 2229-5518 https://www.ijser.org/researchpaper accessed on January 5, 2019
v. Goettke, A & Christiana, J. (2007) "Privacy and online social networking websites," Comput. Sci. 199r Spec.Top. Comput. Sci. Comput. Soc. Priv. Technol..
vi. Hanus B, Wu YA. (2016) Impact of Users? Security Awareness on Desktop Security Behavior: A Protection Motivation Theory Perspective. Information Systems Management.; 33(1):2±16. https://doi.org/10.1080/10580530.2015.1117842
vii. Harris,R.D (2013). "Privacy on the go, recommendations for the mobile ecosystem," Attorney General California Department of Justice.
viii. Internet Penetration In Cameroon, https://www.statista.com/statistics/640127/cameroon-Internet-penetration/
ix. Korolova, R. Motwani, S. U. Nabar, and Y. Xu, "Link privacy in social networks," in Proceedings ofthe 17th ACM conference on Information andknowledge management, 2008, pp. 289–298.
x. Liang, H. & Xue, Y.(2009) Avoidance of information technology threats: a theoretical perspective. MIS quarterly. p. 71±90.
xi. Liang, H. & Xue, Y. (2010) Understanding security behaviors in personal computer usage: A threat avoidance perspective. Journal of the Association for Information Systems.; 11(7):394.
xii. Lipford, H. R., Besmer, A. & Watson, J. (2009). Understanding Privacy Settings in Facebook with an Audience View. Department of Software and Information Systems University of North Carolina
xiii. Luo, W., Xie, Q & Hengartner, U. (2009). "FaceCloak: An Architecture for User Privacy on Social Networking Sites."
xiv. Network Sites: A Case Study of Facebook," Public Policy, pp. 265–273, 2008.
xv. Pitt LF, Parent M, Junglas I, Chan A, Spyropoulou S. (2011) Integrating the smartphone into a sound environmental information systems strategy: principles, practices and a research agenda. The Journal of Strategic Information Systems; 20(1):27–37.
xvi. Ross PE. (2011) Special report: top 11 technologies of the decade. IEEE Spectrum; 48(1):23–27
xvii. Saint, N. 2010. Facebook's Response to Privacy Concerns: "If you're not Comfortable Sharing, Don't". [online]. Available at: http://www.businessinsider.com/facebooks-response-to-privacy-concerns-if-youre-not-comfortable-sharing-dont-2010-5
xviii. [Accessed 8 April 2018]
xix. Scott Mensch, (2016). "Cell Phone Security: Usage Trends and Awareness of Security Issues," Proceedings of International Academic Conferences 3305776, International Institute of Social and Economic Sciences
xx. Tsai HyS, Jiang M, Alhabash S, LaRose R, Rifon NJ, Cotten SR. (2016) Understanding online safety behaviors: A protection motivation theory perspective. Computers & Security.; 59:138±150. https://doi.org/10.1016/j.cose.2016.02.009
xxi. Young, A.L. Na, C & Quan-haase, A. (2008) "Information Revelation and Internet Privacy Concerns on Social
xxii. Zheleva, E. M., Terzi, E., & Getoor, L. (2012). Privacy in social networks. San Rafael, CA: Morgan & Claypool.