Social Networking User Sites and Their Implication on Personal Security of Dagoretti North Constituency Residents in Nairobi County

M. A. M’maka, P. Mwaeye, and E. Bor

ABSTRACT

This study was necessitated by the rising wave of insecurity in the posh places of Nairobi County including in the gated areas that this study presupposed was linked to information shared in social networking user sites. The study was guided by three objectives; to identify the features of online interaction in social networking user sites and their implication on personal security of Dagoretti North Constituency residents in Nairobi County, to identify personal security risks associated with interaction on social networking user sites; and to establish the risk mitigation measures that cushion social networking users in Dagoretti North Constituency in Nairobi County, Kenya. The study adopted a cross-sectional survey design. Questionnaires were used to collect data from 378 members of public while Key Informants (K.I) guide were used to collect qualitative data from 10 K.I who comprised of; police officers in crime branch sections of Kilimani and Kawangware police stations. Stratified random sampling technique was used to pick the main respondents. Data was analyzed with the aid of Statistical Package for Social Sciences (SPSS) and results presented using descriptive statistics. Qualitative responses were presented in verbatim quotes and selected comments. According to this study, Instagram (61.9%), Facebook (48.7%), Google+ (42.1%) and Twitter (31.5%) were the most frequently used sites, used every day. The study concluded that; social media sites expose user’s geographical coordinates, allow the use of pseudo names and credentials that disguise the criminals making them difficult to apprehend, made it easy to find victims with just a few keystrokes, allows replication of information and conceal originality, and hence predisposes user’s credentials to theft. The different features of social media networking sites exposed users to major personal security risks such as abductions, rape, robberies, break-ins, murders and burglaries. In order to address the personal security risks brought about by disclosure of personal identifiable information on social networking sites on the users, the study recommended policy formulation through the ICT ministry to create mechanisms for reaching out to SNS users for purposes of user education on safe usage of SNS. Further, as a matter of policy, the government should benchmark with developed countries for advanced preventive regulations measures against social networking vulnerability hence cushion and protect SNS users.

Keywords: Personal Security, Social Networking User Sites, Social Networking Vulnerability

I. INTRODUCTION

According to Ungerer (2012), social networking user sites have today become the epicenter of social connection and interaction around the world between states, organizations, businesses and individuals. Besides, online social networks have impacted every field of human endeavor from education to health care, polity and religion amongst others. Further, Aday et al. (2010) also argued that the advancement in social media has increased the activities of criminals to the detriment of both national and international security. That notwithstanding, Little attention has however been given to the impact it has had on personal or individual security. This study therefore aims at unveiling the current state of the situation regarding interaction and linkages on social media sites in Kenya and its threats and risks to personal security, hence the rationale for this study.

Social network sites (SNSs) are networked communication podiums where, users have unique and distinguishable profiles comprising of material provided by the user, the system or fellow users (Ellison & Boyd, 2013). The SNSs which include media like Twitter, Facebook, WhatsApp, Instagram, twitter and
Google+ amongst others provide its users opportunities to disclose their information, regarding hobbies, jobs held, movements, family members/relationships and other personal information inextricably intertwined with customized activities/content in order to stay competitive, also keeping audiences interested (Lawler & Molluzo, 2011). According to this study however, personal information shared in such public communication podiums exposes the users or people around them to endanger their lives and property.

According to Rohani and Hock (2009), social networking sites and services offer users a space where they can maintain their relationship, users are required to submit a profile containing personal information such as their full names, date of birth, as well as profile photos. This personal information is made available to other users who have signed up and are using the system, and is used to identify friends on the network and to add them to an existing list of contacts. In some of the systems, users cannot not only view their friends but also second degree friends, who are the friends of their friends. Other networks follow an invitation only’ approach where users have to accept or decline to be added on to the existing contact lists.

The implication here is that public display of connections in SNSs enabling other viewers to traverse the network graph by clicking through the friend lists. According to Liu and Ying (2010), most SNSs also provide a mechanism for users to leave messages on their friend’s profiles. This according to Liu and Ying (2010), make it possible for people to form online communities, and share user-created contents (UCCs). The people may be the users of the open internet or may even be restricted to those who belong to a particular institution or organization such as corporation, professional society, university. The community may be a network of offline friends whose connection is extended to online, online acquaintances, or one or more interest groups based on hobbies, schools attended, profession, gender, ethnicity, age group, cause or interests. The user-created content may comprise of videos, photos, bookmarks of web pages, user profiles, user’s activity updates and engagements, text (comments, micro blogs and blogs). The sharing of the content includes at the minimum viewing, posting, and commenting of the created content, and may also extend to voting on, retransmitting and saving of the content.

In a published article by the US federal government, on Privacy and Security in a connected world, commonly referred to as “The Internet of Things” (IoT), it was argued that information explosion through the use of internet has had implication on security of many states. Rose et al. (2015) defines Internet of Things as a situation where one is able to connect to the internet, Global Positioning System (GPS) and other everyday activities through the use of simple internet enabled objects far away from computers and with minimal human intervention. It can generally be argued that IoTs, have increased the amount of personal data we upload and share with the world by automating a big percentage of the process of tagging and saving images, routes, likes and predicting trends; this potentially raising threats to security (Rose et al., 2015).

According to Chennamaneni and Taneja (2015) Social networking sites and applications have grown astronomically albeit with detrimental security implications. As postulated by Druggan and Brenner (2013) social media accounted for 67% of all internet users while Facebook takes the lead, with a massive turnaround of close to 1.39 billion memberships. Despite email remaining a common hotspot for cyber criminals, this trend seems to be shifting swiftly to the social media platform. A report released by Internet Security Threat Report in 2015 showed that close to about 70% of social media scams were manually scanned. Considering that these scams have the ability to spread rapidly, they often present perfect opportunities to cybercriminal to strike as most people just click thinking it is a common post from their friend.

According to the statistics released by 29 police forces in England, Scotland and Wales under the Freedom of Information Act in 2012, Social networking crime was comparatively minor in 2008 with 556 reports made to police. However, in 2011, the number of reports dramatically increased to 4,908 incidents in which Facebook and Twitter demonstrated an upsurge of crimes by 780% in four years, resulting in approximately 650 people being charged in 2011. The National White Collar Crime Center (NW3C) provides a list of crimes linked to social media; burglary, phishing & social engineering, malware, identity theft, and cyberstalking (National White Collar Crime Center, 2013).

That notwithstanding, most previous scholars such as Fokes and Li, (2014) amongst others mainly focused on other aspects of hardware or devices security while significant others focused on data security. Little attention has been given to online user’s security (Albrechtslund, 2013). Fokes and Li, (2014) categorized security threats of social media into three: (1) platform related, (2) user related, and (3) cyber-attacks (Fokes & Li, 2014). Platform related threats include the network related intrusions, authentication processes, and data breaches while User related threats present vulnerable practices by social media users, including information sharing, privacy coping behavior, alterations on user’s privacy settings. Further, according to Fokes and Li (2014) cyber-attack threats refer to number of dangers such as user’s awareness of social media risks for example spoofing and clickjacking, and attacks of malwares and Trojans. This study will however generally focus on the online user’s personal security.

According to Social bakers (2013) Kenya is the one of the most active country in social networking on
social media platforms in Africa. For example, in 2013 alone Kenya posted 2,476,800 tweets both by individuals and companies making it the second most active country on social networking site on twitter. Top five brands that use Facebook in Kenya are Safaricom Kenya Limited, Samsung Mobile Kenya, OLX Kenya, Midcom East Africa and Airtel Kenya respectively while the top five Kenya Brands on Twitter are Safaricom Limited, Kenya Airways, Safaricom Customer Care, IEBC and Samsung Mobile Kenya (Social bakers, 2013). Whereas Alqubaiti (2016) argued that Social media sites imposed security vulnerability to communities, he did not explicitly specify the type of vulnerabilities and how the community gets affected. Though the National White Collar Crime Center (2013) report linked social media information vulnerabilities to only community burglaries, sudden rise of other crimes in the community especially murders and other homicides more so at the gated areas of Dagoretti North Constituency in Nairobi County, Kenya has been worrying trend that this study presuppose is linked to information theft that link the victims to insecurity, hence, the rationale for this study.

II. PROBLEM ANALYSIS

As argued by Ungerer (2012), the advancement in social media has increased the ability of criminals to not only impact national but also international security. Most previous studies that tried to scratch this area mainly focused on other aspects of hardware or devices security while significant others focused on data security. Little attention has been given to online user’s security and its implication on personal security. The Kenya police service has observed an explained sudden rise of community crimes such as murders and other homicides especially at the gated areas of Dagoretti North Constituency in Nairobi County, a phenomenon that this study attributes to information theft from victims of insecurity, hence, the rationale for this study. Given that most of the social media users remain unknown and cannot be easily traced by law enforcement agencies and subsequent prosecution, states therefore are faced with tough challenges to track, monitor and contain the use and misuse of social media relative to state and personal security. National security demands a strategy such as monitoring conversations and content shared on Social Media, arranging effective methods to counter adversaries’ operations and activities and improving governmental agencies and institutions ‘or strengthening a state’s organizational credibility and effectiveness to counter such online criminals in order to provide security to all citizens.

III. METHODOLOGY

This study adopted a cross-sectional survey design paradigm to investigate the vulnerability of social networking user sites and its implication on personal security of Dagoretti North Constituency residents, specifically, in Kilimani and Kawangware wards because of rising cases of murders, abductions, robberies and burglaries in the area (Kenya Police Service Annual Report, 2018). The questionnaires and Key informant’s interviews were used to collect data. All participants in the study were assured of confidentiality and privacy. Personal identifiers such as names were not included in the data during the course of the study. The participants were also informed before their participation that there would be no direct material or financial benefits for their participation.

The study applied Fisher’s formula (Cochran, 1963) to approximate the sample size. The sample size was derived by computing the minimum sample size required for accuracy in estimating proportions by considering the standard normal deviation set at 95% confidence level (1.96), percentage picking a choice or response (50% = 0.5) and the confidence interval (0.05 = ±5).

$$n = \frac{z^2 (p)(1 - p)}{c^2}$$

$$n = \frac{1.96^2 (0.5)(1-0.5)}{0.05^2} = 384$$

Therefore, a sample of 384 respondents was selected for the study.

The study adopted stratified sampling method to select the key respondents for this study. The procedure involved the development of strata based on the existing mutually exclusive subgroups that comprise the study such that Kilimani respondents formed their own stratum while Kawangware respondents also formed their own stratum. Responses from the two strata were then compared and controlled for Age, Gender, Education, and Employment status of respondents. Besides, Kenya National Bureau of Statistics (KNBS) (2019) statistics registers were used as sample frames for selecting study respondents. Simple random sampling was then used to select respondents for the study. Each ward was thus required to produce 197 respondents.
Quantitative data was analyzed with the aid of Statistical Package for Social Sciences (SPSS Version 25). Descriptive statistics, such as frequency distribution tables, percentages, pie charts and graphs, were used to show details of analyzed data. Qualitative data was presented using verbatim quotes from the respondents.

IV. RESULTS AND DISCUSSION

A total of 378 duly filled and usable questionnaires out of 384 were obtained from respondents for the study. This represented 98.4% response rate and a non-response rate of 1.6%. According to Mugenda and Mugenda (2003), this was sufficient for doing the analysis. Table I below shows the response rate. Therefore, all the tables and graphs presented in this chapter have a sample size of 378 unless stated otherwise. In this regard, some tables have a total response of more than 378 and this represents multiple response (where respondents were required to give more than one response).

<table>
<thead>
<tr>
<th>TABLE I: RESPONSE RATE</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Frequency</strong></td>
</tr>
<tr>
<td>Responded</td>
</tr>
<tr>
<td>Did not respond</td>
</tr>
<tr>
<td><strong>Total</strong></td>
</tr>
</tbody>
</table>

Source: Author (2021)

A. Demographic Information

This section presents demographic information of respondents namely: gender, age, education, residence and employment status of the respondents.

Gender of respondents

From the figure below, over half of the respondents were male (56%) while 44% were female.

![Gender of respondents](image)

Age of respondents

As shown in Fig. 2 almost half (47.9%) had 31 to 40 years of age, 31.0% had 18 to 30 years of age, 15.3% had 41 to 50 and just 5.8% had 51 to 60 years.

![Age of respondents](image)

Education
The study also sought to establish the level of respondents’ education. This was to give the researcher an idea on the level of comprehension on the questions and subject of discussion. As illustrated in the Fig. 3, a majority of the respondents (70.1%) had attained a tertiary level of education while 29.9% had reached secondary level of education.

**Fig. 3. Level of education of respondents**

### Residence

The localities from which the study participants were recruited included Kawangware and Kilimani. Figure below shows that Kawangware had the higher number (52.1%) of respondents while the rest (47.9%) came from Kilimani.

**TABLE II: RESIDENCE OF RESPONDENTS**

<table>
<thead>
<tr>
<th>Residence</th>
<th>Frequency</th>
<th>Percentage %</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kawangware</td>
<td>197</td>
<td>52.1</td>
</tr>
<tr>
<td>Kilimani</td>
<td>181</td>
<td>47.9</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>378</strong></td>
<td><strong>100.0</strong></td>
</tr>
</tbody>
</table>

Source: Author (2021)

### Employment status of respondents

Fig. 4 below illustrates the employment status of the respondents. This was important as it would give the perpetrators a better understanding of their targets.

**Fig. 4. Employment status of respondents**

Based on results on Fig. 4 above, majority of the respondents (58%) had formal employment, 26% were self-employed while only 16% were unemployed.

**V. DISCUSSION OF THE FINDINGS**

### A. Features of Online Interaction in Social Networking User Sites

The study's first objective sought to identify the features of online interaction in social networking and their implications on personal security on users. In order to understand and respond to the objective, the study focused on the social networking sites that respondents use, frequency of using the social networking
sites, characteristics of the social networking sites, as well as the implications on personal security of the respondents. The results indicated that Google+, Facebook and Instagram were the most used social networking sites while Friendster and Myspace were the least used sites. These findings concur with the Statistica (2016) results that identified Facebook as the most popular SNS. Wilson et al. (2012) portended that one possible reason for Facebook’s success was based on the human drive to form social bonds and to communicate. The findings further revealed that WhatsApp and Tiktok were the other popular and most recent sites to have a huge number of users across the world. The study findings also indicated that most of the respondents used Facebook, Instagram, Google+ and Twitter on a daily basis. Myspace and Friendster were the only social network sites that were never used by many of the respondents. LinkedIn was used often as the respondents indicated that they used it at least once per week.

Generally, according to this study, disclosing information on social networking sites enhances traceability of the users and exposes them to unforeseen danger. The study looked at the characteristics of the SNS and it was evident that geographical coordinates of users were acquired on most of the sites, users could use pseudo names and credentials, replicate information and conceal originality while victims could be found with just a few keystrokes. A location taken with a Global Positioning System as a common tagging feature of social Networking sites can ascertain and pinpoint exact position and or if stationary or mobile through constant live feed of longitude and latitudinal coordinates, giving away real time actionable position and whereabouts of a user to potential criminals that pose a great threat to a user’s personal security. Further, perpetrators can also use geographical coordinates to trace their target or their property, making it easy to break into residences when their target indicates to be somewhere else.

According to this study, the use of Pseudo names and credentials, hoodwinked unsuspecting users to give their credible and confidential information (including bank details) that led to huge financial losses through fraud. The owners of these pseudo accounts engage in cyber bullying other social media users taking comfort in the hidden/false identity.

B. Risks Associated with Social Media Use by Operators in Social Networking User Sites

The second objective of the study sought to identify personal security risks associated with interaction on social networking user sites. The findings indicate that nearly all the respondents agreed that there was a relationship between social media use and the threat to personal security. They acknowledged that despite SNS creating a revolution in social connectivity, con artists, criminals and other dishonest actors are exploiting this capability for nefarious purposes. This lends support to Kumar et al. (2016) argument that, by utilizing SNS, people open themselves to different sorts of dangers and insecurity.

The study highlighted abductions and thefts as the major personal security risks as well as rape, robberies, breakings, murders and burglaries. Among the two areas of study, Kawangware emerged as the area with most of these cases when compared to Kilimani. Some of the most common offences in Kawangware included abductions, theft and robberies. On the other hand, Kilimani had cyber bullying, rape, kidnapping, breakings, identity theft, murders and fraud as the most common offences. Sexual harassment was equally experienced in both areas.

As argued by Rose et al. (2015), identity theft continues to affect millions of people across the globe, costing victims’ countless hours and money in identity recovery and repair. Identity theft is a crime in which an imposter obtains key pieces of personal information such as social security numbers in order to either, impersonate someone else and use such information to commit criminal activities Chipurici (2016) The implication here is that with limited government oversight, industry standards or incentives to educate users on security, privacy and identity protection, users are exposed to identity theft and fraud. The study findings further concur with the work of Chipurici (2016) who argues that, apart from crimes such as bullying, stalking, harassing that take place on social media sites, identity Theft has a greater impact on victims compared to the others. Elsevier (2016) adds that social networking sites like Facebook, Twitter, LinkedIn have penetrated so deeply into the lives of anyone, who just has basic knowledge about the use of the Internet. Little do they know that these platforms have become a breeding ground for criminals and especially identity thieves that according to this study may lead to hardened crimes like violent crimes and assassinations.

C. Risk Mitigation Measures to Cushion Social Networking Users

According to this study, only 20% of the respondents had taken risk mitigation measures to cushion themselves from social networking user dangers. They had not displayed details of personal or financial documents in SNUs and also turned off automatic login features as part of the most common mitigation measures. These findings are in line with what was recommended by Irshad and Soomro (2018) by through a list of several raft measures to cushion victims of online users that include; to non-display of confidential or financial documents. They further suggested that documents with personals details on them, be blurred out of names and numbers.

The use of automatic login was also mentioned by Mali (2013), who emphasized the importance of turning off automatic login in as an effort to prevent those who illegally access the device do not view any
personal information. Some of the other common mitigation measures suggested by this study included the use of strong and unique passwords and enabling alerts of unusual activity in the user accounts, use of protection services such as identity guard and life, avoiding geo-tagging photos and not posting of location updates as well awareness talks at both organizational and community levels.

This is emphasized by both Smith (2014) and Mali (2013) who suggest that Posting of Location Updates should also be avoided as it gives the criminals solid information on victim whereabouts. The study suggested Setting Stringent Privacy Settings in light of the fact that one’s personal information such as name, photo, date of birth, location, place of work etc. are sensitive data, so that such information is just useful to only themselves or to people they trust.

VI. CONCLUSION AND RECOMMENDATIONS

The study concluded that, Social media sites expose user’s geographical coordinates, allow the use of pseudo names and credentials that disguise the criminals making them difficult to apprehend, made it easy to find victims with just a few keystrokes, allows replication of information and conceal originality, and also predisposes user’s credentials to theft. Further, the study established that there is a relationship between social media use and the threat to personal security. The different features of social media networking sites exposed users to major personal security risks as abductions, rape, robberies, breakings, murders and burglaries.

According to the study, some of the other common mitigation measures include the use of strong and unique passwords and enabling alerts of unusual activity in the user accounts, use of protection services such as identity guard and life, avoiding geo-tagging photos and not posting of location updates as well as awareness talks at both organizational and community levels.

In order to address the personal security risks brought about by disclosure of personal identifiable information on social networking sites on the users, the study recommended policy formulation and recommendation through the ICT ministry to create mechanisms for reaching out to SNS users for purposes of user sensitization on safe usage of SNS. Further, as a matter of policy, the study recommends mandatory settings in SNS that can enable users to limit the amount of personal data that third-party applications can access. SNS just give automatically ticked options of what these apps can access. The study also recommends mandatory awareness inductions in learning institutions that proactively incorporate security awareness inductions or formulate additional curriculum that sensitize especially the youth who are the majority of SNS users on the need to be personally aware of the security threats posed by SNS and subsequently on the best practices while engaging in SNS interactions.

National Government Administrative Officers i.e. (The County Commissioners, Deputy County Commissioners, Chiefs and Assistant chiefs) to sensitize the communities during public Baraza’s can adopt the same approach. Further, as a matter of policy, the government should benchmark with developed countries for advanced preventive regulation measure’s against social networking vulnerability hence cushion and protect SNS users.

CONFLICT OF INTEREST

Authors declare that they do not have any conflict of interest.

REFERENCES


Ungerer, C. (27 February 2012), Social Media and National Security, ASPI Strategic Policy Form.