SOCIAL NETWORKING USER SITES AND THEIR IMPLICATION ON PERSONAL SECURITY OF DAGORETTI NORTH CONSTITUENCY RESIDENTS IN NAIROBI COUNTY, KENYA

MOHAMED ABDUL M'MAKA

A Thesis Submitted to the Graduate School in Partial Fulfilment of the Requirements for the Master of Arts Degree in Security Management of Egerton University

EGERTON UNIVERSITY

DECEMBER, 2022

DECLARATION AND RECOMMENDATIONS

Declaration

This thesis is my original work and to the best of my knowledge has not been presented for examination of any Degree or Diploma in any institution or university.

Date: December, 2022

M'MAKA ABDUL MOHAMED

AM21/0217/12

Recommendation

This thesis has been submitted for examination with our recommendation as university supervisors.

Signature……... **Date: December 2022**

Prof. Eric Bor, Ph.D

Department of Peace, Security and Social Studies

Egerton University

Signature…… **Date: December 2022**

Dr. Panuel Mwaeke, Ph.D

Department of Peace, Security and Social Studies

Egerton University

COPYRIGHT

DEDICATION

To my wife Johra, dear children; Maysam and Minha, My Parents Abdul Mzee and Badrie Omar, other family members, friends and colleagues. To my children, may this work be an inspiration for you to reach greater heights in academics.

ACKNOWLEDGEMENTS

I acknowledge the goodness of the Almighty God for granting me life; good health and understanding that enabled me undertake this work.

I acknowledge my supervisors; Prof Erick Bor and Dr. Panuel Mwaeke for their scholarly comments, guidance and sincere criticism, which helped shape my research work, and without whose support, this work would be incomplete. I remain greatly indebted to them.

I am grateful to my wife and children for their constant concern and moral support. I also acknowledge my employer and colleagues at work for their moral, and emotional support towards this important academic achievement and milestone.

I am indeed indebted to the officers in the people of Dagoretti North Constituency residents in the jurisdictions of Kilimani and Kawangware Ward for giving me the much needed support to conduct the research and for giving me the information that was needed in this study. To my research assistant, kindly accept my gratitude for the support during and after the fieldwork.

I acknowledge all persons who contributed to the success of this work, though I may not mention each one of you, kindly accept my appreciation. Thank You.

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. This study was grounded by the Protection motivation theory and 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. Some of the features of online interaction in social networking user sites identified by this study include; exposing user's geographical coordinates, permit use of pseudo names and credentials that disguise criminals making them difficult to apprehend, made it easy to find victims with just a few keystrokes, and finally allow replication of information and conceal originality, hence predisposes user's credentials to theft. According to the study 53.8% of the respondents in Kawangware reported to have been crime victims compared to 39.8% of the respondents in Kilimani area. These differences were statistically significant (p=0.05). The different features of social media networking sites exposed users to major personal security risks such as abductions, rape, robberies, breakings, 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 social media networking site (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.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS AND ACRONYMS

CAK: Communication Authority of Kenya

DCI: Directorate of Criminal Intelligence

FERF: Financial Executives Research Foundation

GPS: Global Positioning System

IEBC: Independent Electoral and Boundaries Commission

IoT: The Internet of Things

K.I: Key informants

KNBS: Kenya National Bureau of Statistics

NACOSTI: National Commission for Science, Technology and Innovation

OCPD: Officer Commanding Police Division

SNSs: Social network sites

SPSS: Statistical Package for Social Sciences

CHAPTER ONE
INTRODUCTION

1.1 Background to the Study

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. In addition, 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 unveiled 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 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, and family members / relationships and other personal information with customized activities /content in order to stay competitive and keep audiences interested (Lawler & Molluzo, 2010). As was established through this study such personal information sharing in public communication podiums exposed the users or people around them and endangered their lives and property.

American psychologist Stanley Milgram (1967) in his work ‘small world experiment’, in which he sent letters to sixty volunteers in Kansa and asked them to forward the envelopes to a specific person in Massachusetts by hand and through friends or friends of friends. According to the experiment, the letters that reached the addresses were, on average, relayed by five to seven people. This is seen as an empirical proof that arbitrary people in our society are related to each other though friends and friends of friends. The small world hypothesis, based on Milgram’s findings states that the number of personal acquaintances needed to connect two random persons on the planet is small. The hypothesis led to the expression ‘the six degrees of separation’, meaning that any two random persons are associated with each other by a chain of

about six individuals. Therefore, the 'six degrees of separation' is one of the underlying concepts of social networks on the internet.

According to Rohani and Hock (2009), social networking sites and services offer users a space where they can maintain their relationship, converse with each other while sharing information. Furthermore, they offer the opportunity to develop new relations through existing friends. In the beginning of adoption, users are required to submit a profile containing personal information such as their full names, date of birth, as well as a profile photo. 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 public display of connections is a crucial component of SNSs. The friends list contains links to each friend's profile, 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 feature typically involves leaving comments'. Furthermore, these sites often have a private messaging feature similar to webmail.

Kim (2010) defined the social websites as those sites that 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, and 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. Roughly, Won Kim regards social web sites as a union of networking sites and social media sites.

Social network sites are defined by Boyd (2007), as 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.

The nature and nomenclature of these connections may vary from site to site. This study recognizes that the terms ‘social networking sites’ and ‘social media sites’ have been previously loosely and widely used in the press blogs, articles, press releases from the sites and the features of such sites continue to rapidly evolve. Therefore, we do not feel that efforts to define social networking sites more precisely than above are warranted. Roughly, social networking sites are web sites that allow users to stay connected with other people in online communities. Some of the most widely used social networking sites include Facebook, Twitter, Instagram, Google+, WhatsApp, Tiktok and Tinder. Since their introduction, social networking sites (SNS) have attracted millions of people in the world, who have integrated these sites into their daily life. SNSs continue to connect people based on different features with different technologies. Despite the extent to which they vary, SNSs have fairly consistent key features, by which can help the development of these sites and their practices in electronic commerce.

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. According to a study by Druggan and Brenner (2013) social media accounted for 67 % of all internet users. Additionally, Facebook takes the lead, with a massive turnaround of close to 1.39 billion. Membership. 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's 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 has 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 Joinson *et al.* (2010) and Gacy (2010), amongst others focused on other aspects of hardware or devices security and significant others 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, authentication processes, and data breaches while User related threats present vulnerable practices by social media users, including information sharing, privacy coping behavior, the preventable user, user's privacy settings, and lack of privacy awareness. 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.

In Kenya, a report gathered from Safaricom, the largest mobile service provider in Kenya and the largest devices retailer occupying over 85 % of the mobile data market share, by Communication Authority of Kenya (CAK) (2016) revealed that Consumer purchase of Smartphones is currently at 67 % over the total phone sales. This unprecedented growth in smartphone use means that the number of Kenyans connecting to new media like Twitter, Facebook, WhatsApp, Instagram, twitter and Google+ has also increased. Despite such revelation, there is little has been done about user's privacy and or their security implication.

Additionally, according to Social bakers (2013), there are 1,886,560 registered Facebook users in Kenya and Kenya ranks sixth in Africa in terms of population usage of Facebook. Furthermore, a report titled "How Africa Tweets" by Portland Communications and Tweet mister suggests that in the last quarter of 2011, Kenya posted 2,476,800 tweets making it the second most active country on the social networking site twitter. As a result of the popularity of social media in Kenya, top 5 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 (Socialbakers, 2013).

Socialbakers (2013) further aver that the most commonly used social media platforms in Kenya are Facebook, Twitter. 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 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 an appalling phenomenon that this study assumes is linked to information theft that link the victims to insecurity, hence, the rationale for this study.

1.2 Statement of the Problem

Social networking user sites have today become the epicenter of social connection and interaction around the world between states, organizations, businesses and individuals albeit with security implications. Besides, the advancement in social media has increased the ability of criminals to not only impact national but also international security. Few documented studies that scratched this area tried to link social media information with vulnerabilities at community level through crimes such as burglaries. This area has however, never been subject of a systematic inquiry and investigation, more so in Kenya. Besides, the National Police Service Annual Reports revealed a sudden rise of other crimes in the community especially murders and other homicides especially at the gated areas of Dagoretti North Constituency in Nairobi County, Kenya which this study assumed and later established was linked to information theft from victims of insecurity. This study at the onset, this study presupposed and later established

that criminals use social media social networking user sites to send alarming messages, intimidate, effect surveillance on other people to either kill or main them. This is exacerbated by the fact that most of the social media users remain unanimous 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 security. It is therefore imperative that National security moots 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 and effect personal security to all citizens.

1.3 Objectives of the Study

This study was guided by both broad and specific objectives as follows;

1.3.1 Broad Objective

The broad objective was to assess the vulnerability of social networking user sites and its implication on personal security of Dagoretti North Constituency residents in Nairobi County, Kenya.

1.3.2 Specific Objective

This study was guided by the following study objectives

i. 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, Kenya.
ii. To identify personal security risks associated with interaction on social networking user sites in Dagoretti North Constituency residents in Nairobi County, Kenya.
iii. To establish the risk mitigation measures to cushion social networking users in Dagoretti North Constituency in Nairobi County, Kenya.

1.4 Research Questions

i. What are the features of online interaction in social networking user sites and their implication on personal security, in Dagoretti North Constituency residents in Nairobi County, Kenya?

ii. Which are personal security risks associated with interaction on social networking user sites in Dagoretti North Constituency residents in Nairobi County, Kenya?

iii. Which are risk mitigation measures that can be used to cushion social networking users of Dagoretti North Constituency residents in Nairobi County, Kenya?

1.5 Justification of the Study

This study sought to assess the vulnerability of social networking user sites and its implication on personal security of Dagoretti North Constituency residents. It is expected that the study findings may generate new knowledge and inform policy formulation and recommendation with regard to personal security in Kenya.

This study has generated new knowledge that will benefit Law enforcement agencies by enhancing their operation efficiency. Business community will also benefit from improved business ambience and finally the citizens through improved personal security. This will include reduced personal attacks, Murders, Abductions, robberies, and frauds amongst other personal security threats.

The findings of this study may provide unique strength to security agencies as an operational guide in understanding the key dynamics and trade-offs that may inform their operational procedures with regard to Social network sites

Finally, as it was also anticipated findings of this study will address knowledge gaps and be used as a basis for further scholarly work and research.

1.6 Scope and Limitation of the Study

Even though this study was set to assess the vulnerability of social networking user sites and its implication on personal security of Dagoretti North Constituency residents, this study was limited to Kilimani and Kawangware wards only. This is despite the fact that Dagoretti North Constituency has five wards, Kilimani, Kawangware, Gatina, Kileleshwa and Kabiro. Kilimani and Kawangware wards were chosen because of certain characteristics considered desirable for this study in that the two study sites were used to represent perceptions of the Middle class (Kilimani) and those of the relatively lower class (Kawangware).

Additionally, given that the Dagoretti North Constituency has about 180,000 respondents, generalizing findings from a sample size of 384 respondents only may be a serious limitation.

Besides, due to the sensitivity of the study problem to security, some of the respondents with crucial information may not be free to share it. This may as a result be an impediment to the study. However, this kind of challenge was overcome meticulously by seeking informed consent from all the respondents. The researcher explained to the respondents that the information will be treated with confidentiality and will only be used for academic purposes and for the improvement of the personal security to residents of Dagoretti North Constituency.

1.7 Definition of Terms

Social Networking User Sites: In this study, this term has been used to mean media like Twitter,

Facebook, WhatsApp, Instagram, and Google+, LinkedIn, etc

Features of Online Interaction: In this study, this term has been used to mean unique characteristics that predispose users to personal security risks for example, ability to acquire the geographical coordinates of users, Easy finding of victims, Replicability: networked public expressions can be copied from one place to another verbatim such that there is no way to distinguish the "original" from the "copy."; and Invisible audiences: inability to detect most people who can catch up with your private information while unnoticed. Impossibility to ascertain all those who might run across victim expressions in networked publics.

Risks Associated with Social Media: In this study, this term has been used to mean criminal activities such as Abductions, Murders, Thefts, Burglary and breakings etc.

Personal insecurity: In this study, this term has been used to mean Abductions, Murders, Thefts, Burglary and breakings, Robberies, Frauds etc.

CHAPTER TWO
LITERATURE REVIEW

2.1 Introduction

This chapter reviews all available literature from past studies on vulnerability of social networking user sites and its implication on personal security of the users. First the chapter will assess literature on known features of online interaction in social networking user sites and their implication on personal security. Secondly, this section looks at the various risks associated with social media use by users in SNSs. Thirdly, literature about known risk mitigation measures to cushion social networking users will be discussed. Finally, the chapter looks at various theoretical frameworks underpinning the study. Based on this review, knowledge gaps in the current state of literature are discussed.

2.2 Features of Online Interaction in Social Networking User Sites

Previous scholars such as Al-Daghir (2013), Byrne (2008), Charnigo and Barnett-Ellis (2007), Hargittai, (2008), Humphreys (2008), Kim and Yun (2008) Lange (2008), Spertus *et al. (*2005) and Stutzman (2006) on SNS mainly focuses on their use by individuals, groups and features of the software applications themselves. Very little has been done on security implication or consequences of interactions on SNSs cites. This study assumes that the occurring interplay between users, user agency and the software architecture, which can be argued to play a central role in shaping the actual outcomes in terms of networking processes and activities, related to SNSs should not be overlooked. Further, Boyd and Ellison (2008) portended that SNSs are "web-based services that allow individuals to either; construct a public or semi-public profile within a bounded system, or articulate a list of other users with whom they share a connection, and finally view and traverse their list of connections and those made by others within the system" (boyd & Ellison, 2008).

According to Boyd (2007) teenage use of popular SNSs, such as Friendster and MySpace, Boyd (2007) argues that SNSs are characterized by three basic properties common to mediating technologies: persistence, replicability and invisible audiences. However, in the author's view, "networked publics add an additional feature-*searchability* –while magnifying all of the other properties" (Boyd, 2007). Boyd (2007). As far as persistence is concerned the ephemeral quality of speech in unmediated publics, networked communications are recorded for posterity

Boyd (2007). This enables asynchronous communication but it also extends the period of existence of any speech act.

Another feature of communications in SNSs is complexity of searchability; implying that people cannot currently acquire the geographical coordinates of any person in unmediated spaces. Additionally, with replicability networked public expressions can be copied from one place to another verbatim such that there is no way to distinguish the "original" from the "copy." According to Boyd (2007) other feature include invisible audience, where most people can overhear speeches in unmediated spaces, though virtually impossible to ascertain all those who might run across those expressions in networked publics. This is further complicated by the other three properties, since Online expression may be heard at a different time and place from when and where they were originally made (Boyd, 2007).

This establishment of a virtual identity controlled through profile building is therefore seen as crucial in defining SNS, together with the articulation of connections with other virtual identities that represent the virtual audience whereby channels of communication can be developed. Studies on impression management and friendship performance focus on processes initiated by the online representations of self that are enabled by SNSs (Donath & boyd, 2004; Fono & Raynes-Goldie, 2006; Skog, 2005). A characteristic that emerges as crucial is therefore the degree of control over user profiling allowed by different SNSs. Drawing on data gathered through ethnography and reaffirmed through data collection and visualization, Boyd and Heer (2006) analyze the use of profiling features in Friendster, concluding that virtual profiles in SNSs play a central role in context creation and interpretation, negotiating unknown audiences, and initiating conversations. A number of contributions focus on the privacy issue raised by SNS diffusion (Preibusch *et al.*, 2007). Gross and Acquisti (2006) carry out a survey study on privacy awareness and privacy concerns among Facebook users, concluding that while users voice their privacy concerns, they do not behave accordingly, exerting only lose control over their personal information (Gross & Acquisti, 2006).

Boyd (2007), Choi (2006), Lampe *et al.* (2007) and Steinfield (2007) further aver that the network building activity, which results from the interaction between the digital personas, as a consequence, also plays an important role in defining core characteristics of SNS. Findings by Choi (2006) further point out that the main motivator for the use of SNS is to maintain and reinforce existing social networks in the offline world. Relatedly, Lampe *et al.* (2007) show

how a SNS like Facebook is actually not used for establishing new social networks, that is meeting new people online, but primarily to solidify existing social relations. In their opinion, this specific feature is the one that differentiates SNSs from previously existing online applications such as, for instance, newsgroups. Regarding the network structure topic area, a large scale analysis of Facebook messaging (Lampe *et al.*, 2007) points out the role of transaction costs reduction in explaining the number of links (or "friends") within SNS user nodes. A reduction in transaction costs can thus also be identified as a key factor of network maintenance activated through SNS. Boyd (2007) underlines the characteristics of persistence in how SNSs maintain networks, observing that "unlike the ephemeral quality of speech in unmediated publics, networked communications are recorded for posterity. This enables asynchronous communication but it also extends the period of existence of any speech act". Liu *et al.* (2006) and Liu (2008) underline how SNSs activate links that go beyond the formal "friendship" connections provided by the software applications, and develop an alternate network of tastes, which links individual users with each other.

Kim and Yun (2008) focus on the way a SNS's design features and functions encourage users to transcend the interpersonal principles they imply in face-to-face interaction. They observe how users of a Korean SNS routinely negotiate multiple dialectical tensions that are created within the online world, transferred from face-to-face contexts, or shaped by culture. Breslin and Decker (2007) draw on Knorr-Cetina's concept of "object-centred sociality" (Knorr-Cetina, 1997) in arguing that SNSs' unique characteristic is the capacity of linking individuals around shared content, rather than just of providing simple connections without any intermediate objects –such as, for instance, multimedia content. Based on a longitudinal analysis of the development of SNSs in trying to sketch the future evolution of SNSs, they point out that so far the main feature that distinguished a successful SNS from an unsuccessful one has been its focus on content. Les successful sites, they argue, "act simply as enhanced address books" (Breslin & Decker, 2007). The evolution of SNSs will increasingly move toward bringing users together around shared objects (e.g.: photos on Flickr, job information on LinkedIn, video clips on YouTube, music on Last.fm, etc.), making *object-centeredness* the SNSs' main characteristic.

As has already been argued elsewhere virtual profiles in SNSs play a central role in context creation and interpretation, negotiating unknown audiences, and initiating conversations, a number of contributions focus on the privacy issue raised by SNS diffusion (Preibusch *et al.*,

2007) but did not factor personal safety and or security in configuration. Additionally, Gross and Acquisti (2006) in their study carried out a survey on privacy awareness and privacy concerns among Facebook users, concluding that while users voice their privacy concerns, they do not behave accordingly, exerting only lose control over their personal information (Gross & Acquisti, 2006). This study takes this argument a notch higher by exploring the effect of privacy gaps in SNSs and its implication on personal security in the Dagoretti North constituency, in Nairobi County, Kenya.

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

Logging into someone else's account for intentional misuse has become quite common nowadays and so has Identity theft, where fake accounts or accounts for impersonation are made solely for the purpose of fraud. Chipurici (2016) 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. Social networking sites like Facebook, Twitter, and 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 (Elsevier, 2016).

Laudon *et al.* (2010) avers that 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 (Laudon *et al.,* 2010). While in many cases, this information is shared in posts, photos and profiles published on social media sites, the user's ability or inability to control access to this information posted on the social media sites has been a source of controversy. According to Vander (2008), 25% of social media users cannot find security settings provided by social media sites leaving them at the mercy of the default settings on these sites. The lack of transparency on the social media service provider on what information is being shared and with whom, a lack of user controls to provision access to their posts, as well as misconfigured privacy settings can all expose users to inadvertently sharing of personal or confidential employee and corporate credentials which may enable hackers to obtain answers to standard security challenge questions (BITS, 2011).

Black *et al.* (2014) portended that the users of the social networking websites share various information and in the process lose privacy when they share their important and personal information with strangers. Additionally, it has also been noticed that sharing of information

with the strangers have led many users to fall in honey traps. Hence, one of the most important concerns that have emerged with the usage of the social networking websites is insecurity. Arguably, it has been reviewed that most of the users are basically unaware of the fact about the various security risks that are prolifically involved with the sharing of sensitive information on the social networking websites. It is quite important that the users must know that the default settings on these websites actually share every bit of personal information (Black *et al.*, 2014). Even today, the primary purpose of Identity Theft has not changed, but only methods of intrusion and platforms have transformed. Some of the ways that were being used years ago and are still adopted for acquiring personal information are listed below:

2.3.1 Phishing

Phishing refers to a kind of fraud in which the criminal tries to gain access to personal information, such as account information or login credentials by impersonating as a trusted entity. This usually performed by two methods. First sending links of fake Websites that capture your login and password credentials and second by becoming friends with the person by sending false acquaintance messages, which the person unknowingly accepts (Hoelscher, 2017). Further, Experian (2010) argued that on social networking sites, this is accomplished by sending requests to play a Quiz, complete a survey or share something for a free giveaway (Experian, 2010).

2.3.2 Social Media Cons and Hacking

This is a common scheme, which fraudsters use on Facebook, where they steal someone's identity and send out plea messages for cash to that person's friends and family. Concerned family and friends get tricked and send out money to these criminals (Experian, 2010). Besides, through Identity Spoofing; criminals create fake accounts of musicians, politicians, and actors etc. to gather sensitive data from other people or in hopes to tarnishing their image (Hoelscher, 2017). On the other hand, in the case of hacking, victims use the same password for almost all accounts. Once the hacker gets access to your social accounts, they can easily get hold of your bank account data, online shopping details, and credit card details or even use your social accounts to perform criminal activities (Hoelscher, 2017).

2.3.3 Spamming

What comes in different forms, 'spamming' refers to an indecent process that involves the sharing of unwanted messages. In most of the cases, it's mode of propagation are the emails.

According to Kandikanti (2017), there might be a single person or a group of many such people that send irrelevant messages. Such people are called spam attackers or spammers. While this process of spamming is enabled only through electronic media, social networking sites are the ultimate destination for spammers. Spamming attacks continue to bring a kind of realization that social networking media are not really reliable when it comes to issues concerning spamming. Spammers can easily make their way into the account of other people. In a very convenient and secretive way, they hack accounts and share unsolicited messages and links to the user's contacts that mostly comprises of relatives and friends. When a friend or follow request is accepted by the user, things turn easy for a hacker who ca now tour through the user's account and gain information.

2.4 Risk Mitigation Measures to Cushion Social Networking Users

Risk management is the evaluation of potential risks and development of strategies to reduce the risks and learn about future risks. It involves risk identification including probabilities and impact, identification of possible solutions to the risks, implementation of the solutions and risk monitoring to learn future risk assessment (Chaffey & Wood, 2005). The rise of social media should not be considered isolated or unique but rather an evolution of online communications with special considerations when used in a very broad and public setting and whose control requirements may not be unique but may be challenged given the ways technologies are deployed (BITS, 2010). For many companies, social media is the proverbial double edged swords offering opportunities and risks cutting across many areas of the company including HR, marketing, communications, legal among others and while no one can foresee all the risks, they must be anticipated in order to be properly addressed (FERF & Thornton, 2011). Social media risks can be mitigated in the following ways.

2.4.1 Social Media Management Framework at Individual Level

Social media has no doubt created an atmosphere and culture of unnecessary sharing and publicizing of personal information which should be kept hidden most of the time. This has eventually led criminals of Identity Theft to tap into these data and cause financial losses. Although sites like Facebook, Twitter etc. have taken considerable steps to curb the issue of online theft and protect user's privacy, it still remains a challenge for these organizations to allow them to share and interact limitlessly without pushing them to become victims of fraud (Lawrence, 2016). As the trend of exploiting personal information is on the rise, it is important

to take precautions on the user's end to avoid getting noticed and becoming victims to online identity theft.

Irshad and Soomro (2018) suggested several raft measures to cushion victims of online users that include; to never display details of personal or financial documents: They argued that this is something that criminals of identity theft are mostly looking for to steal identities. They further suggest that documents with personals details on them, be blurred out of names and numbers. Besides, online users should always turn off Automatic Login Features. As argued by Mali (2013) Never allow social media application to auto log you in and also don't allow browsers to remember your log in details. In case if someone gets hold of your device, they won't be able to directly gain access to your account. Thus, preventing them from viewing your personal information (Mali, 2013).

Both Mali (2013) and Smith (2014) suggested that Posting of Location Updates should also be avoided. When user's post about their vacations and whereabouts online, it gives the criminals solid information that they are going to be out of their homes at the time of update thereby allowing the thieves to break in and steal valuables or more importantly identifying documents to be used for impersonation (Mali, 2013).

Scholars such as Myhre (2013) recommended 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. This can be done by going into the settings of Facebook, Instagram, LinkedIn, Twitter accounts and changing the preferences for your personal data. Additionally, Drager (2011) recommended the Use of Strong and Unique Passwords; that are strong, secure and unique such as making them alphanumeric with special characters helps in keeping identity thieves at bay.

Others measures include; Always Connecting with Authentic People; Using Double Authentication; For example, Twitter allows users to turn on a setting that asks users to enter a one-time code sent to their mobile phones when they log in for the first time from a particular device; Avoid Using Same Passwords for Multiple Accounts; Never Keeping Credit Card Information Online; Avoid Geo-Tagging Photos; Use of Protection Services such as Identity

Guard and Life Lock provide solutions against identity theft for safeguarding your social media accounts. If one feels they need professional services to protect their accounts, these services are the way to go; and Enabling Alerts of Unusual Activity in user accounts.

2.4.2 Social Media Management Framework in the Organization

FERF and Thornton (2011) argue that employers should approach social media and social networking tools from a social media policy perspective for its effective and efficient management. The same argument is fronted by BITS (2011) that a clearly posted and well communicated social media policy around the usage of social media on and off network is one of the most important risk mitigation measures. Chellia and Field (2012) link social media policy and the employees‟ contracts in risk mitigation by reiterating that an employer's position could be strengthened by having a clearly defined internal grievance procedure as well as a well-defined policy on the use of social media that refers back to the employment contract and stresses that posting negative comments about the organization and work colleagues is not acceptable.

FERF and Thornton (2011) however caution that because social media cuts across many areas of a company like marketing, HR, legal, communications among others, any policy surrounding it must be the result of a multidisciplinary approach. Chellia and Field (2012) detail this further by stating that if employers are serious about managing social media risks in their organizations then they must get serious about developing a well-coordinated human resource management strategy that not only includes documented policies and procedures but also an internal training program and robust record keeping procedures. In addition to an all-inclusive approach stated above, BITS (2011) encourage companies to develop policies that are narrowly tailored and not overly broad. The policies must balance the employer's needs to protect themselves and the employee's right to a personal existence and voice as well as reference other related policies such as code of ethics, internet usage, and info security.

2.4.3 Risk Communication

According to Pattinson and Anderson (2007), the manner in which people see risks associated with information security determines what decisions they will make regarding the actions they will take (or not take) in conjunction with whatever security measures their organization has put in place. They outline that one of the factors purported to have an influence on risk perception is the way in which a risk message is communicated to computer end users and

management. Bener (2000) claims that the manner in which risk is communicated within an organization substantially influences the risk perception of the different individuals within that organization. Lipa (1994) voiced the same opinion that an individual's perception of risks is shaped by the way in which risky situations are communicated to them within a particular context.

Pattinson and Anderson (2007), identify security awareness seminars, standard email memos, notice board memos, phone calls, web pages, one on one discussions, group meetings and flyers as some common forms of risk communication. However, they propose that together with these information security messages, symbols and graphics would improve the effectiveness of risk communication in the organization and the general perception of the risks to the information systems would be more realistic.

2.5 Summary of Literature review

Personal security risks associated with interaction on social networking user sites here in refers to Abductions, Murders, Thefts, Burglary and breakings amongst others that this study is set to study. All these forms of crimes can be done easily because when an attacker hacks an account, he is accessible to the user's personal information. And sometimes he gains the user's identity, his address, picture and other information too. So stealing, robbery and their allied forms become easy. Physical damages can be easily facilitated. The user never knows or gains knowledge of the hacker. On the other hand, anonymity provides a favorable condition in social networking websites for identity theft by hackers or attackers and not for the users or victims who really do are not aware of their consequences.

According to Bilton (2010) a very common practice among social media users is to post their vacation statuses on their pages for their friends and family to see, but some of them leave these statuses as public for everyone to see. This makes them an easy target for burglars to rob their houses, when they are away on vacations. In his study, he found that three local men who were arrested on charges of burglary of more than 18 houses in New Hampshire confessed that they used social networking sites to target their victims. It is upon this backdrop that this study is set to collect data and assess the vulnerability of social networking user sites and its implication on personal security of Dagoretti North Constituency residents in Nairobi County, Kenya.

2.6 Theoretical Framework

This study was guided by the Protection Motivation Theory (PMT). The theory was useful as it tried to predict measurable relationships between the vulnerability of users' information on SNSs and their personal security.

2.6.1 Protection Motivation Theory

This study was guided by Protection motivation theory. This theory founded by Rogers (1975) argued that "an individual's intention to protect him or herself depends on four factors: (1) the perceived severity of a threatening event; (2) the perceived probability of the occurrence; (3) the efficacy of the recommended preventive behavior that an individual expects to carry out; and (4) the individual's perceived self-efficacy" (Chai *et al.,* 2009; Rogers, 1975).

The PMT underlines two processes to predict and mediate protection motivation: threat appraisals and mitigation appraisals (Kaspar, 2015). Threat appraisal evaluates the severity level of an activity/situation and examines how serious it is (Rogers, 1983), in this case personal security threats. Conversely mitigation appraisal evaluates (response- efficacy) of adapting a protection behavior (Kaspar, 2015), where in efficacy the individual's (Online users in social media platforms) are expected to carry out or comply with recommendations or mitigation measures that can remove the threat and according to this study lessen the threat of personal insecurity against residents at of Dagoretti North Constituency residents (Rogers, 1983).

This study assumed that using different social Media sites make users to experience a variety of online security threats that require them to enact safety precautions. In this study, PMT has been used as a powerful model to understand and predict the adoption of protective technologies, and one of the main theoretical foundations in the information security research field, which helps users avoid harm from a growing number of negative technologies by practicing healthier behaviors when dealing with security issues (Boss *et al.,* 2015; Chenoweth *et al.,* 2009).

This study used PMT to understand online safety behaviors in the context of social media use and mitigate on resultant threats. For example, in a previous research, Jenkins *et al.* (2014) provided two solutions to limit password reuse through detection and mitigation, based on

PMT. Secondly, in an investigative study of the influence of fear appeals on the compliance of end users, Johnston and Warkentin (2010) pointed out the effect of fear appeals in the end user behavior when responding to a recommended act of security.

This study used the four factors of PMT: (1) the perceived severity of a threatening event; (2) the perceived probability of the occurrence; (3) the efficacy of the recommended preventive behavior that an individual expects to carry out; and (4) the individual's perceived self-efficacy" to predict measurable relationships between the vulnerability of users' information on SNSs and their personal security.

2.7 Conceptual Framework

Basically, the conceptual framework shows relationship between the constructs (variables).

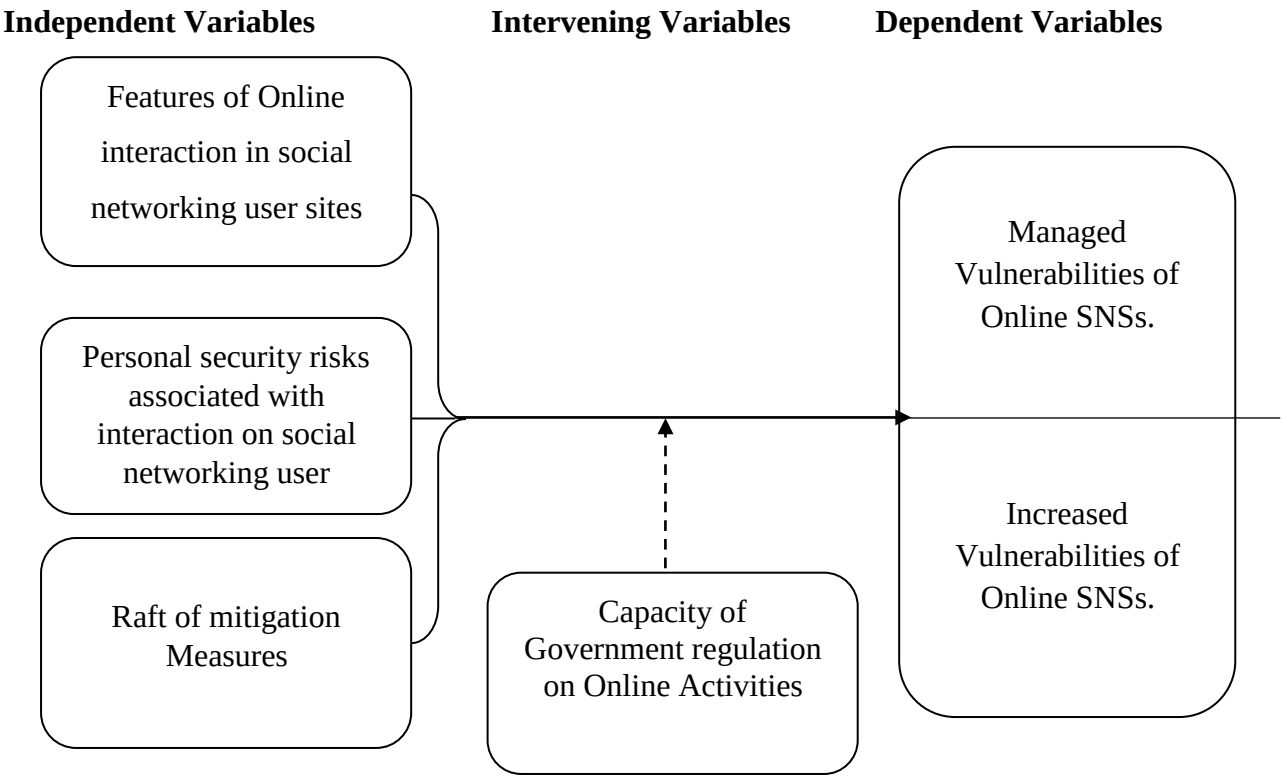

Figure 2.1: Conceptual Framework

The conceptual framework above describes the relationship between independent variables and dependent variables. If there is strengthened government capacity to check on online user sites (intervening variables) then resident's personal security will be enhanced. Conversely in the event of weak government capacity then the result is increased vulnerabilities of Online SNSs.

CHAPTER THREE
METHODOLOGY

3.1 Introduction

This chapter describes the methods that was used to meet the objectives of the study. The chapter describes; site of study, target population, research design, sample and sampling procedure, methods and tools of data collection, and methods of data analysis.

3.2 The Study Design

This study adopted a cross-sectional survey design. This was due to the need to have a comprehensive coverage of the phenomenon under study; to assess the vulnerability of social networking user sites and its implication on personal security of Dagoretti North Constituency residents in Nairobi County, Kenya.

3.3 Study Area

This study was conducted in Dagoretti North Constituency in Nairobi County, Kenya. According to the National Population Census (2019) Dagoretti North Constituency has a population of 180,000 people spread across five wards namely; Kilimani, Kawangware, Gatina, Kileleshwa and Kabiro. This study was however conducted in Kilimani and Kawangware wards because of rising cases of murders, abductions, robberies and burglaries in the area (Kenya Police Service Annual Report, 2018) which this study attributes to personal information stolen from social networking user sites. The Map of the study site is presented in Figure 3.1.

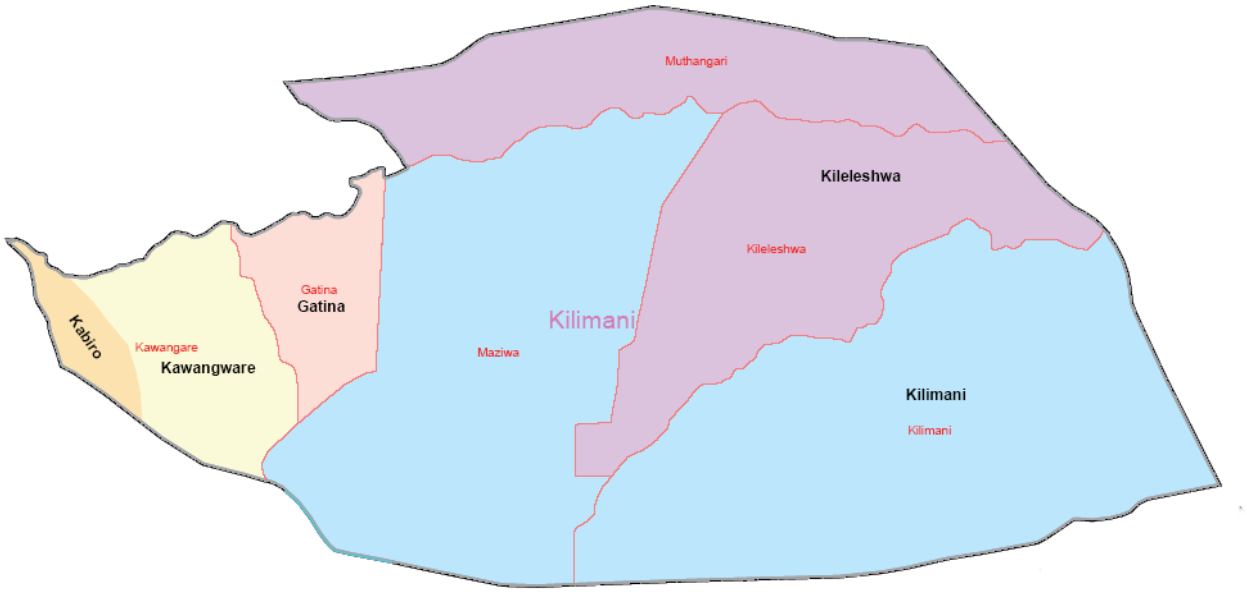

Figure 3.1: Map of the Study Site

3.4 Target Population and Sampling Procedure

According to the National Population Census (2019), Dagoretti North Constituency has a population of 180,000 people spread across five wards namely; Kilimani, Kawangware, Gatina, Kileleshwa and Kabiro.

Due to the huge target population of the study area, Fisher's formula (Cochran., 1963; Gorstein, 2007) was applied 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). The formula is:

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

Where:

n = sample size

z = standard normal deviation set at 95% confidence level

p = percentage picking a choice or response

c = confidence interval

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

$$= 0.9604 / 0.0025$$

$$= 384.14$$

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.

3.5 Unit of Analyses

The unit of analysis was the residents of Kilimani and Kawangware**,** in Dagoretti North Constituency, in Nairobi County, Kenya. In addition, opinion of K.I who comprised of; police officers in crime branch section at Kilimani police station and Kawangware police, DCIO and OCPD of that jurisdiction were also analyzed.

3.6 Methods and Tools of Data Collection

The study used both Questionnaire and Key informants (K.I) interview method to collect data.
Questionnaires were used to collect data from main respondents (Residents of Kilimani and Kawangware) while K. I schedules were used to collect data from the K. I's (Police officers in crime branch section at Kilimani police station and Kawangware police, DCIO and OCPD of that jurisdiction).
Questionnaires adopted both structured, semi structured and unstructured questions to collect data. The nature of questions gave the respondents the freedom to decide on the form, detail and length of their answers. In addition, these questions helped to gain more insight and knowledge that this study may not have anticipated.

3.7 Data Analysis

Data collected was collated, organized, summarized and interpreted systematically and thematically. Qualitative responses were presented in verbatim quotes and selected comments. Descriptive statistics were utilized to analyze the quantitative data. Descriptive statistics, in particular, included; measuring the relative frequencies, central tendency, frequency distribution tables, and variability. Tables and diagrams were used to show details of analyzed data. Quantitative data was analyzed with the aid of Statistical Package for Social Sciences (SPSS Version 25).

3.9 Ethical Consideration

This study sought consent from respondents before it was executed. Respondents were assured of their anonymity and confidentiality and that information they gave would solely be used for research purposes. Approvals to carry out research were obtained from Egerton University Board of Postgraduate Studies, from the National Commission for Science, Technology and Innovation (NACOSTI) and from the Nairobi County Commissioner.

CHAPTER FOUR
RESULTS AND DISCUSSION

4.1 Introduction

This chapter presents findings of the study based on research objectives. Primary data was collected through questionnaires and analyzed using descriptive statistics of frequencies and percentages. The data was further thematically organized based and presented in graphically to show the relationships amongst study variables.

4.2 Response Rate

A total of 378 dully 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 4.1 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 4.1: Response Rate

	Frequency	***Percentage %***
Responded	378	98.4
Did not respond	6	1.6
Total	**384**	**100**

4.3 Demographic Information

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

4.3.1 Gender of respondents

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

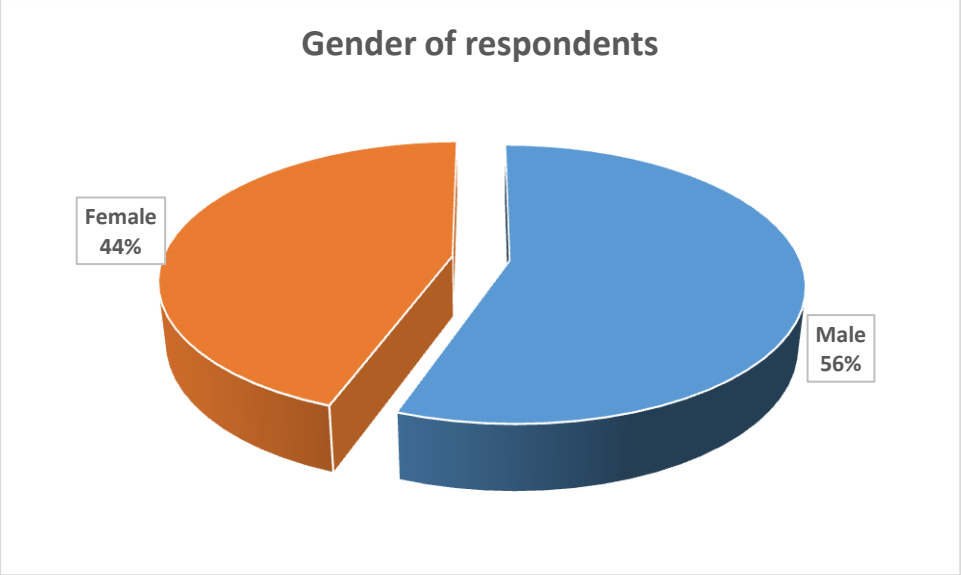

Figure 4.1: Gender of respondents

4.3.2 Age of Respondents

Figure below indicates that 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.

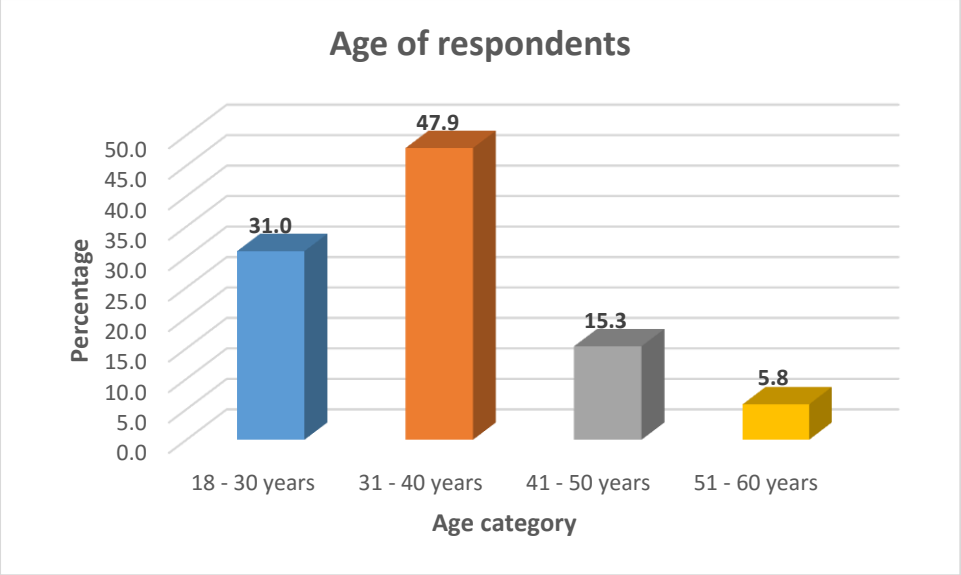

Figure 4.2: Age of respondents

4.3.3 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 figure below, a majority of the respondents (70.1%) had attained a tertiary level of education while 29.9% had reached secondary level of education.

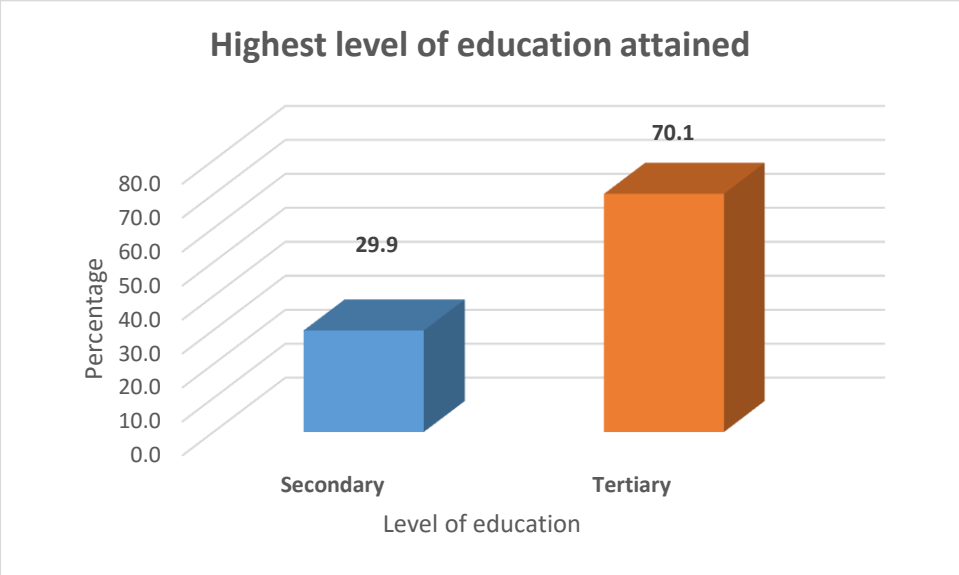

Figure 4.3: Level of education of respondents

4.3.4 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 4.2: Residence of respondents

	Frequency	***Percent***
Kawangware	197	52.1
Kilimani	181	47.9
Total	**378**	**100.0**

4.3.5 Employment status of respondents

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

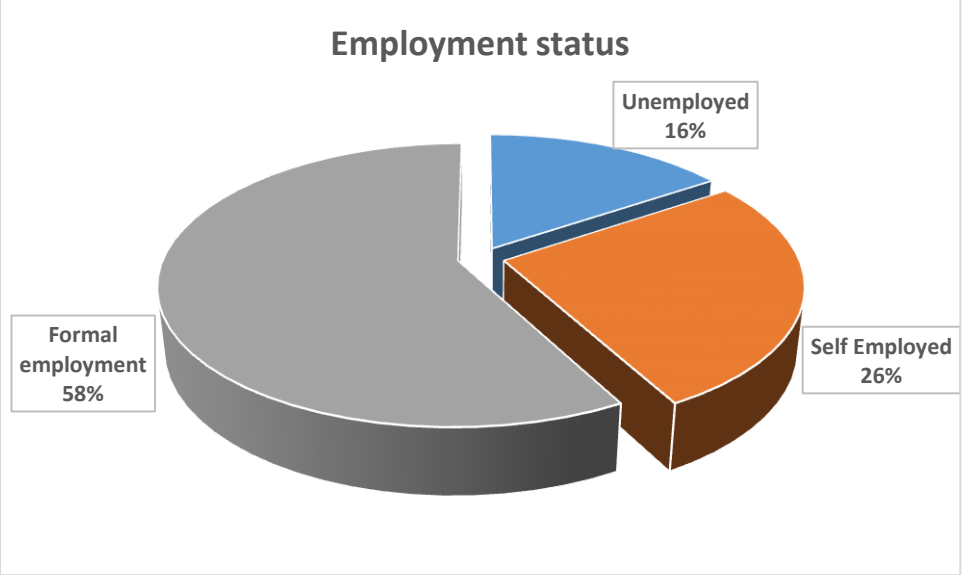

Figure 4.4: Employment status of respondents

Based on results on Figure 4.4 above, majority of the respondents (58%) had formal employment, 26% were self-employed while only 16% were unemployed.

4.4 Results

The findings of this study were organized based on the objectives as follows.

4.4.1 Features of online interaction in social networking user sites and their implication on personal security

The first objective of the study sought to identify the features of online interaction in social networking and their implications on personal security on users. Under this objective, the study focused on the social networking sites that respondent's 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.

Social networking sites that respondents use

The respondents were asked to point out the social networking sites they use and results were as illustrated in Figure 4.5.

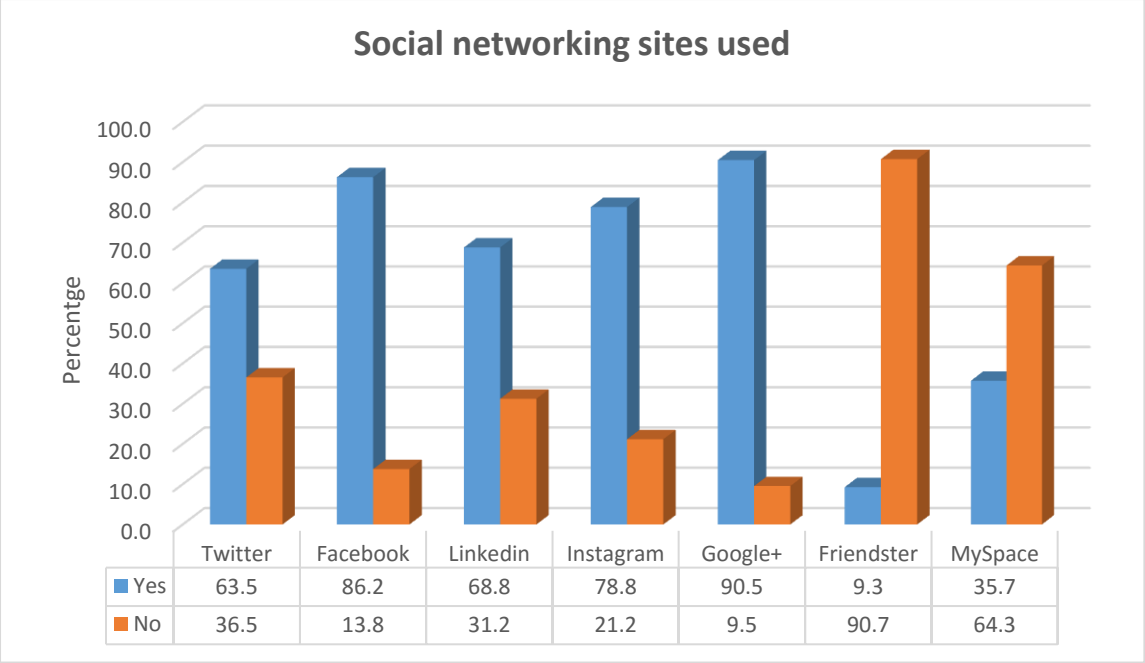

Figure 4.5: Social networking sites used

The results indicated that most of the respondents used Google+ (90.0%), followed by Facebook (87.0%), Instagram (79.0%), LinkedIn (69.0%), and Twitter (64.0%). On the other hand, most of the respondents did not use Friendster (90.0%) and Myspace (65.0%) as indicated in the table below.

The researcher also asked the respondents to mention any other social networking sites they use beyond the ones that were initially listed. A majority of the respondents mentioned WhatsApp (86.2%), followed by Tiktok (19.2%), snapchat (6.0%) and Tinder (2.4%) as shown in the figure 4.6 below.

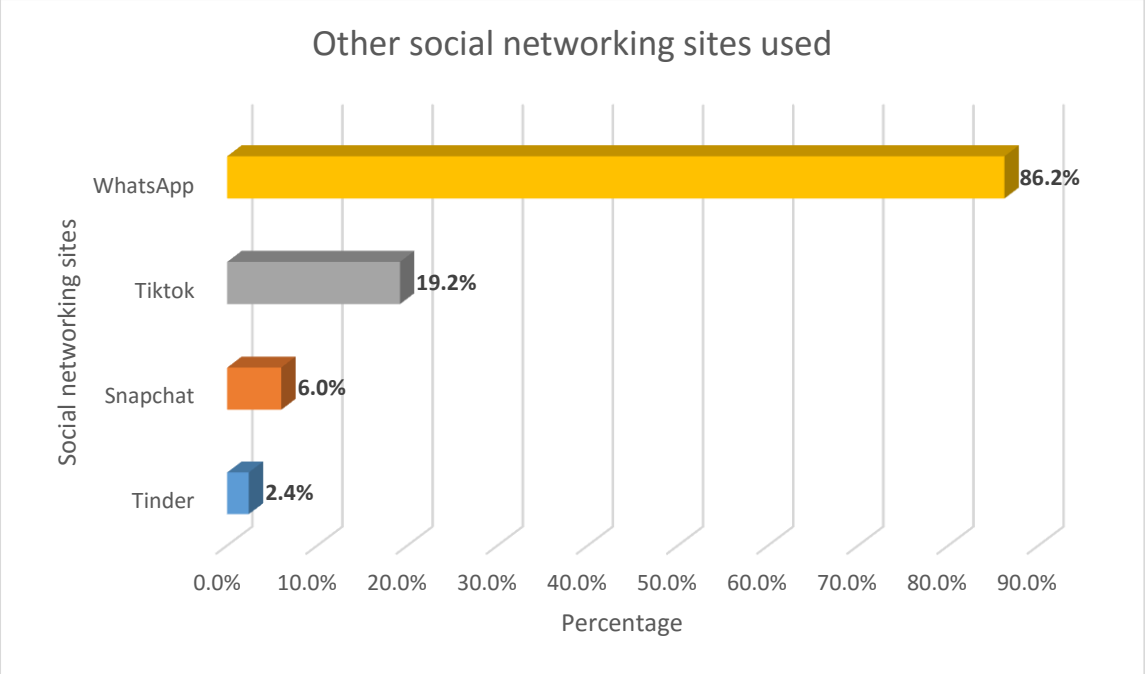

Figure 4.6: Other social networking sites used

Frequency of using social networking sites

The study also sought to identify the frequency of using the social networking sites by the respondents.

Table 4.3: Frequency of using social networking sites

	Never	***Rarely (Once in a month)***	***Often (At least once a week)***	***Frequently (Everyday)***	***Always (Always Online)***
Twitter	26.7	16.7	18.8	31.5	6.3
Facebook	17.7	13.8	13.5	48.7	6.3
LinkedIn	21.7	28.6	32.8	14.6	2.4
Instagram	14.8	15.9	7.4	61.9	0.0
Google+	20.6	11.9	19.6	42.1	5.8
Friendster	87.8	0.0	6.3	2.4	3.4
Myspace	64.3	13.5	7.4	9.3	5.5

The results indicated that Instagram (61.9%), Facebook (48.7%), Google+ (42.1%) and Twitter (31.5%) were the most frequently used sites as they were used every day while Friendster and Myspace never used by 87.8% and 64.3% of the respondents respectively.

Characteristics of social networking sites

The study further sought to identify the characteristics of the social networking sites. The respondents were asked to identify if the identified features were true or false when it comes to the sites. Their responses were as shown in Table 4.4 below.

Table 4.4: Characteristics of social networking sites

	True	***False***
Acquire geographical coordinates of users	87.6%	12.4%
Use of Pseudo names and credentials	93.9%	6.1%
Find victims with just a few keystrokes	93.9%	6.1%
Replicate information and conceal originality	96.6%	3.4%
Distinguish "originality" from the "copy."	72.0%	28.0%
Steal someone's credentials	89.9%	10.1%
Being Invisible audiences	98.9%	1.1%
Ascertain those who might run across victim expressions in networked publics	75.1%	24.9%

The results indicated that most of the respondents affirmed that the sites acquired the geographical coordinates of users (87.6%), allowed the use of pseudo names and credentials (93.9%), found victims with just a few keystrokes (93.9%), could allow replication of information and conceal originality (96.6%), steal some0ne's credentials (89.9%), ascertain those who might run across victim expressions in networked publics (75.1%) as well as allow being invisible audiences (98.9%).

Comparison with demographic characteristics

The study further sought to explore the dynamics between various demographic characteristics on the opinion about characteristics of social networking sites. Here, perceptions about the various characteristics of social networking sites were cross-tabulated with gender, age, education, residency and employment status of the respondents.

Gender

When respondents' perceptions were cross-tabulated with respondent's gender to explore whether male and female respondents had divergent opinions, the results were as shown in Table 4.5 below.

Table 4.5: Characteristics of social networking sites by gender of respondents

		Gender of respondent		*χ^2-Value*	*df*	*P-Value*
		Male	**Female**			
Acquire geo*graphical coordinates of users*	True	84.8%	91.1%	3.413	1	0.065
	False	15.2%	8.9%			
Use of Pseudo names and credentials	True	89.0%	100.0%	19.592	1	0.000
	False	11.0%	0.0%			
Find victims with just a few keystrokes	True	95.2%	92.3%	1.447	1	0.229
	False	4.8%	7.7%			
Replicate information and conceal originality	True	100.0%	92.3%	16.829	1	0.000
	False	0.0%	7.7%			
Distinguish "originality" from the "copy."	True	71.9%	72.0%	0.001	1	0.980
	False	28.1%	28.0%			
Steal someone's credentials	True	95.2%	83.3%	14.628	1	0.000
	False	4.8%	16.7%			
Being Invisible audiences	True	98.1%	100.0%	3.234	1	0.072
	False	1.9%	0.0%			
Ascertain those who might run across victim expressions in networked publics	True	77.6%	72.0%	1.564	1	0.211
	False	22.4%	28.0%			

Based on the above results, men and women who in Dagoretti North Sub-County had significantly different views of the ability of criminals to use pseudo names and credentials of social networking sites users (χ^2- Value = 19.592, p-value <0.001). In this regard, all the female participants (100%) ascertained that the use of Pseudo names and credentials was a characteristic of social networking sites, an opinion held by 89.0% of the male participants. On the other hand, all the male respondents reported that disclosure of vital information on SNS would enable criminals to replicate information and conceal originality. This opinion, however, was held by 92.3% of the female respondents. The opinion differed significantly (χ^2- Value = 16.829, p-value <0.001). Similarly, the opinions of male and female respondents were significantly divergent with regard to ability of criminals to steal someone's credentials in social networking sites. Here, 95.2% of the male respondents agreed that disclosure of vital information in social media would lead to someone's credentials being stolen compared to only 83.3% of the female respondents who agreed to this assertion. This result was significantly different (χ^2- Value = 16.829, p-value <0.001).

Age

In a similar way, respondents' perceptions on characteristics of social networking user sites were cross-tabulated with respondent's age to explore whether age had an influence on their opinions, and the results were as shown in Table 4.6 below.

Table 4.6: Characteristics of social networking sites by age of respondents

		Age of respondent				χ^2- *Value*	*df*	*P-Value*
		18 - 30 years	**31 - 40 years**	**41 - 50 years**	**51 - 60 years**			
Acquire geographical coordinates of users	True	88.9%	100.0%	41.4%	100.0%	142.65	3	0.000
	False	11.1%	0.0%	58.6%	0.0%			
Use of Pseudo names and credentials	True	100.0%	100.0%	60.3%	100.0%	135.118	3	0.000
	False	0.0%	0.0%	39.7%	0.0%			
Find victims with just a few keystrokes	True	100.0%	92.8%	82.8%	100.0%	22.021	3	0.000
	False	0.0%	7.2%	17.2%	0.0%			
Replicate information and conceal originality	True	100.0%	100.0%	100.0%	40.9%	217.856	3	0.000
	False	0.0%	0.0%	0.0%	59.1%			
Distinguish “originality” from the “copy.”	True	63.2%	84.5%	77.6%	0.0%	75.941	3	0.000
	False	36.8%	15.5%	22.4%	100.0%			
Steal someone’s credentials	True	100.0%	92.8%	56.9%	100.0%	87.251	3	0.000
	False	0.0%	7.2%	43.1%	0.0%			
Being Invisible audiences	True	100.0%	97.8%	100.0%	100.0%	4.4	3	0.221
	False	0.0%	2.2%	0.0%	0.0%			
Ascertain those who might run across victim expressions in networked publics	True	88.9%	81.2%	41.4%	40.9%	64.593	3	0.000
	False	11.1%	18.8%	58.6%	59.1%			

As evidenced in the results on Table 4.6 above, different age categories had divergent opinions on various characteristics of social networking sites (SNSs). For instance, different age categories of respondents had different opinion with respect to ability to acquire geographical coordinates of users as a result of their activities in social media where only 41.4% of respondents aged between 41 – 50 years agreed that criminals were able to get the geographical coordinates of users compared to 88.9% of the respondents between 18 – 30 years and all respondents between 31-40 years as well as those who were above 50 years who had a similar opinion. This difference was statistically significant (p-value < 0.001).

In addition, only 39.7% of the respondents aged between 41 – 50 years held a conflicting opinion from the rest of the respondents with regard to ability to use pseudo names and credentials of users. All other respondents opined that it was possible for criminals to use pseudo names and credentials of users as a result of disclosure of vital information in social media while 39.7% of those aged between 41-50 years refuted this claim. This difference was statistically significant (p-value < 0.001). This was similar to the aspect of ability to find victims with just a few keystrokes where all the respondents said it was true whilst only 17.2% of respondent between ages of 41-50 years and 7.2% of respondents between ages of 31 - 40 years.

Further, all the respondents across the age categories agreed that it was possible for people to replicate information and conceal originality less for 59.1% of respondents who were above 50 years' old who said it was not possible. This difference in opinion was statistically significant (p-value < 0.001). With regard to ability to distinguish "originality" from the "copy", majority of the respondents across other age categories affirmed that indeed it was easy to distinguish originality from the copy apart from all the respondents aged above 50 years who refuted the claim. This divergence in opinion was statistically significant since the p-value was less the alpha value of 0.05. in addition, all respondents agreed that it possible to steal someone's credentials based on the information they post on social networking sites apart from 43.1% of respondent between ages of 41-50 years and 7.2% of respondents between ages of 31 - 40 years. This departure was significant at 95% level of confidence (p-value < 0.001). Finally, more that 80% of respondents between ages of 18 to 40 years agreed that it was possible to ascertain those who might run across victim expressions in networked publics, while only a paltry 40% of those

above 40 years old were in agreement. This difference in opinion was also statistically significant (p-value < 0.001).

Education

Similarly, respondents' perceptions on characteristics of social networking user sites were cross-tabulated with respondent's highest level of education attained to explore whether education had an effect on their opinions, and the results were as shown in Table 4.7 below.

Table 4.7: Characteristics of social networking sites by education of respondents

		Highest level of education		***χ^2-Value***	***df***	***P-Value***
		Secondary	**Tertiary**			
Acquire geographical coordinates of users	True	0.0%	90.7%	94.814	1	0.000
	False	100.0%	9.3%			
Use of Pseudo names and credentials	True	100.0%	93.7%	0.872	1	0.350
	False	0.0%	6.3%			
Find victims with just *a few keystrokes*	True	100.0%	93.7%	0.872	1	0.350
	False	0.0%	6.3%			
Replicate information and conceal originality	True	100.0%	96.4%	0.48	1	0.489
	False	0.0%	3.6%			
Distinguish "originality" from the "copy."	True	0.0%	74.5%	34.547	1	0.000
	False	100.0%	25.5%			
Steal someone's credentials	True	100.0%	89.6%	1.505	1	0.220
	False	0.0%	10.4%			
Being Invisible audiences	True	100.0%	98.9%	0.144	1	0.704
	False	0.0%	1.1%			
Ascertain those who might run across victim expressions in networked publics	True	0.0%	77.8%	40.675	1	0.000
	False	100.0%	22.2%			

Based on the above results in Table 4.7, three characteristics of social networking user sites depicted significantly different opinion among the respondents. For instance, there was a complete divergence in opinion on whether it was possible to acquire geographical coordinates of users based on their activities in social media. Here, all the respondents who had attained at

most secondary school education said it was not possible, a complete departure from those who had tertiary level of education where 90.7% said it was possible. In another scenario, all the respondents with secondary school education reported that it was not possible to distinguish "originality" from the "copy", an assertion refuted by three out of every four respondents who had attained tertiary level of education. Moreover, all the respondents with at most secondary school education disagreed that it was possible to ascertain those who might run across victim expressions in networked publics whereas most of those who had tertiary education (77.8%) agreed that it was indeed possible to ascertain those who might run across victim expressions in networked publics. This divergence in opinion between these two groups of respondents was statistically significant (p-value < 0.001).

Employment status

Besides, respondents' perceptions on characteristics of social networking user sites were cross-tabulated with respondent's employment status to explore whether employment status had an effect on their opinions, and the results were as shown in Table 4.8 below.

Table 4.8: Characteristics of social networking sites by employment status of respondents

		Employment status			χ^2- *Value*	*df*	*P-Value*
		Unemployed	**Self Employed**	**Formal employment**			
Acquire geographical coordinates of users	True	78.0%	90.0%	89.0%	5.976	2	0.050
	False	22.0%	10.0%	11.0%			
Use of Pseudo names and credentials	True	100.0%	91.0%	93.6%	5.346	2	0.069
	False	0.0%	9.0%	6.4%			
Find victims *with just a few keystrokes*	True	100.0%	96.0%	91.3%	7.156	2	0.028
	False	0.0%	4.0%	8.7%			
Replicate information and conceal originality	True	100.0%	100.0%	94.1%	9.775	2	0.008
	False	0.0%	0.0%	5.9%			
Distinguish "originality" from the "copy."	True	35.6%	86.0%	75.3%	49.68	2	0.000
	False	64.4%	14.0%	24.7%			
Steal someone's credentials	True	100.0%	81.0%	91.3%	15.906	2	0.000
	False	0.0%	19.0%	8.7%			
Being Invisible audiences	True	100.0%	99.0%	98.6%	0.837	2	0.658
	False	0.0%	1.0%	1.4%			
Ascertain th*ose who might run across victim expressions in networked publics*	True	61.0%	81.0%	76.3%	8.282	2	0.016
	False	39.0%	19.0%	23.7%			

As evidenced in the results on Table 4.8 above, respondents of different employment statuses had significantly divergent opinions on various characteristics of social networking user sites. To put this into perspective, a larger proportion of the unemployed (22%) agreed that it was not possible for one to acquire geographical coordinates of users compared to 10.0% of the self-employed and 11.0% of the respondents who were in formal employment. With regards to ability to find victims with just a few keystrokes, all the respondent agreed that it was possible whilst for only 8.7% of the formally employed and 4.0% of the self-employed respondents.

Similarly, all the respondents agreed that it was possible to replicate information and conceal originality of information posted on social networking sites apart from 5.9% among the formally employed respondents who significantly differed. In addition, respondents significantly differed in opinion on the aspect of being able to distinguish "originality" from the "copy". Whereas majority of the self-employed as well as those who were formally employed agreed that it was possible to distinguish originality from copy (86.0% and 75.3% respectively), most of the unemployed respondents (64.4%) opined that it was not possible to distinguish between the two.

On the other hand, all the respondents across the employment statuses agreed that it was possible to Steal someone's credentials less for 19.0% of the self-employed and 8.7% of the formally employed who significantly differed from the rest. Further, opinions of respondents across the three employment statuses differed significantly on whether it was possible to ascertain those who might run across victim expressions in networked publics. For instance, 61.0% of the unemployed respondents agreed that it was possible to indeed ascertain those who might run across victim expressions in networked publics, while 39.0% differed. Similarly, 81.0% of the self-employed and 76.3% of the formally employed respondents agreed that it was possible to indeed ascertain those who might run across victim expressions in networked publics, whilst 19.0% and 23.7% of the self-employed and formally employed respectively significantly held a contradicting opinion.

Residence

Besides, respondents' perceptions on characteristics of social networking user sites were cross-tabulated with respondent's residence to explore whether their opinions were influenced by the place they reside in, and the results were as shown in Table 4.9 below.

Table 4.9: Characteristics of social networking sites by residence of respondents

		Residence		χ^2*- Value*	*df*	*P-Value*
		Kawangware	**Kilimani**			
Acquire geographical coordinates of users	True	83.2%	92.3%	7.043	1	0.008
	False	16.8%	7.7%			
Use of Pseudo names and credentials	True	91.9%	96.1%	2.988	1	0.084
	False	8.1%	3.9%			
Find victims with just a *few keystrokes*	True	94.9%	92.8%	0.732	1	0.392
	False	5.1%	7.2%			
Replicate information and conceal originality	True	100.0%	92.8%	14.653	1	0.000
	False		7.2%			
Distinguish “originality” from the “copy.”	True	65.5%	79.0%	8.549	1	0.003
	False	34.5%	21.0%			
Steal someone’s credentials	True	90.4%	89.5%	0.076	1	0.783
	False	9.6%	10.5%			
Being Invisible audiences	True	99.5%	98.3%	1.191	1	0.275
	False	0.5%	1.7%			
Ascertain those who might run across victim expressions in networked publics	True	73.1%	77.3%	0.913	1	0.339
	False	26.9%	22.7%			

Based on the results in Table 4.9 above, only three characteristics of social networking user sites depicted significantly different opinion among the respondents of Kawangware and Kilimani areas. For instance, 92.3% of the respondents in Kilimani area agreed that it was possible to acquire the geographical coordinates of users compared to 83.2% of the respondents in Kawangware area. This difference in opinion was statistically significant at p-value <0.05. Moreover, all the respondents in Kawangware reported that it was possible to replicate information and conceal originality whereas 7.2% significantly contradicted. In addition, most of the respondents in Kilimani (79.0%) and in Kawangware (65.5%) ascertained that it was possible to distinguish “originality” from the “copy” while 34.5% of respondents in Kawangware and 21.0% in Kilimani respectively held a contrary opinion. This divergence in opinion was statistically significant (p-value < 0.05).

Security implications of using social networking sites

The study further sought to establish the implications of disclosing information on social networking sites on personal security of users. The respondents were required to highlight the security implications of each of the characteristics of the social networking sites. Generally, the study established that disclosing information on social networking sites enhances traceability of the users and exposes them to unforeseen danger. It also poses threat to personal security such as abductions, theft and murder. One of the key informants stated:

> *"Everything that we do nowadays especially the younger ones, it is all on social media, I went out, I had fun with my friends, I was at this place, I did this…. You are endangering your safety; you are putting yourself at risk. We know that is the trend… that is the life today… everything little thing you do, you want to post it on social media, you want people to know. There is very high possibility that these kidnappers all they need to do is simply study your profile on social media."*

The ability to acquire geographical coordinates of users enables the perpetrators of crime to get the user's location where a criminal can do surveillance on the victim and possibly get hold of him or her. It was further noted that 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. Moreover, the study revealed that Geographical Coordinates exposes a person's location or whereabouts thus a security threat.

Another respondent said;

> *"Criminals can use geographical coordinates to trace their target or their property or even break into residence when their target indicates to be somewhere else."*

With regard to use of Pseudo names and credentials, the study found out that one may pretend to be someone and in the real sense he is not. This poses a threat as one may be exposed to criminals. It was also revealed that the owners of these pseudo accounts engage in cyber bullying other social media users taking comfort in the hidden/false identity. They also engage as unscrupulous traders who disappear with other people's money. Another finding was that these criminals can be very difficult to arrest and therefore very difficult to police crimes committed by such people.

On the other hand, stealing credentials particularly mobile data may lead hacking of personal accounts and may lead to theft of personal belongings like money in bank accounts. Criminals can also draw funds from mobile wallets and take loans leaving the individual at a loss. It was further noted that when criminals steal user's credentials or use pseudo names, it is difficult to distinguish "originality" from the "copy". In this regard, it is difficult to arrest the real suspects. At times wrong people may end up being victimized and put in jails for offenses they did not commit. Later, spirit of revenge for wrongful confinement leads to more crimes against law enforcement officers.

4.4.2 Personal security risks associated with interaction on social networking user sites

The second objective of the study sought to identify personal security risks associated with interaction on social networking user sites. Under this objective, the study focused on the relationship between social media use and its threat to personal security of users, the personal security risks that users had been exposed to, the common crimes with the neighborhoods of the respondents as well as the link between crime and use of social networking sites.

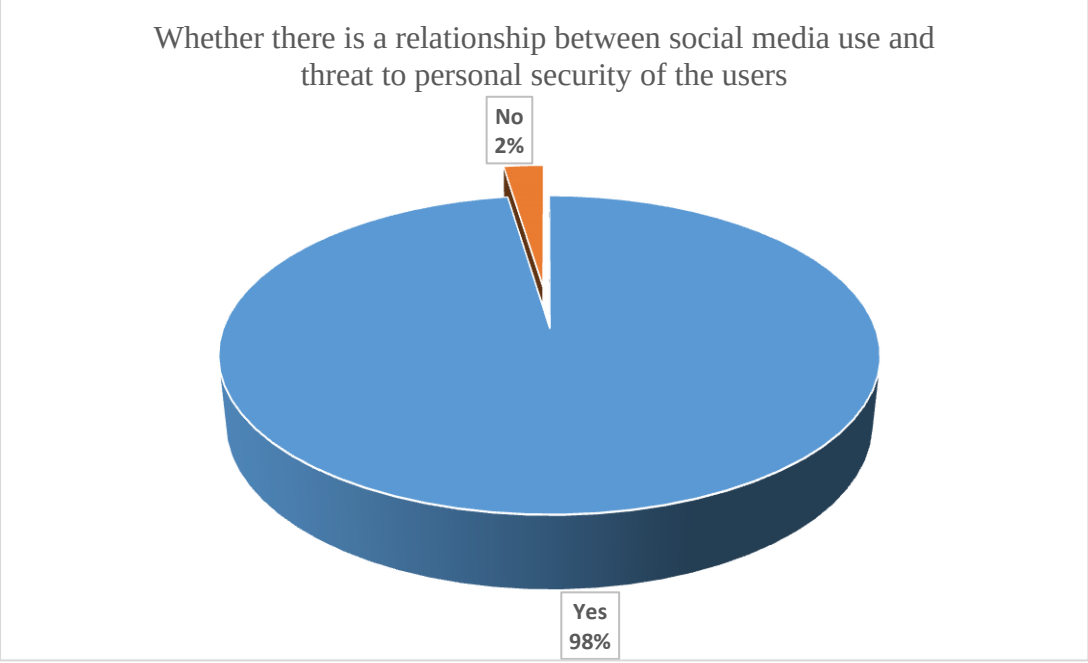

Figure 4.7: Relationship between social media use and threat to personal security of the users

When asked whether there was a relationship between social media use and threat to personal security of the users, nearly all the respondents (98%) agreed with only 2% not agreeing.

Further, the study sought to explore whether there were any differences in opinion across various demographic characteristics of the respondents. Therefore, data on the relationship between social media use and threat to personal security of users was cross-tabulated with the various socio-demographic characteristic. The results were as shown in Table 4.10 below.

Table 4.10: Relationship between social media use and threat to personal security of users vs demographic characteristics

		Relationship between social media use and threat to personal security of users		***χ^2-Value***	***df***	***P-Value***
		Yes	**No**			
Gender	Male	95.7%	4.3%	7.376	1	0.007
	Female	100.0%	0.0%			
Age	18 - 30 years	100.0%	0.0%	149.188	3	0.000
	31 - 40 years	100.0%	0.0%			
	41 - 50 years	100.0%	0.0%			
	51 - 60 years	59.1%	40.9%			
Level of education	Secondary	100.0%	0.0%	0.328	1	0.567
	Tertiary	97.5%	2.5%			
Employment status	Unemployed	100.0%	0.0%	6.694	2	0.035
	Self Employed	100.0%	0.0%			
	Formal employment	95.9%	4.1%			
Residence	Kawangware	100.0%	0.0%	10.034	1	0.002
	Kilimani	95.0%	5.0%			

As evidenced on Table 4.10, results indicate that there were significantly divergent opinions across the various demographic characteristics of respondents. For instance, all the female respondents agreed that there was a relationship between social media use and threat to personal security of users while 4.3% of male respondents held a contrary opinion. With regards to age, all the respondents agreed between 18 – 50 years ascertained that there was a relationship between social media use and threat to personal security of users compared to 59.1% of those aged above 50 years who held a similar opinion. This assertion was also made by all the respondents across the employment cadres apart from 4.1% formally employed respondents

who differed with the rest. Similarly, there was a significant difference in opinions of both Kilimani and Kawangware residents where all Kawangware respondents agreed that there was a relationship between social media use and threat to personal security of users, but 5% of Kilimani respondents contradicted. These differences in opinions were statistically significant (p-value < 0.05).

Personal security risks

Since most of the respondents indicated that there was a relationship between use of social media and threat to personal security of users, the study further sought to establish the most common security risks as a result of information disclosure on social media. The findings were as shown in Table 4.11 below.

Table 4.11: Personal security risks

	Yes	***No***
Abductions	100.0	0.0
Thefts	100.0	0.0
Rape	93.4	6.6
Robberies	92.6	7.4
Breakings	86.8	13.2
Murders	86.0	14.0
Burglaries	84.4	15.6

As evidenced in Table 4.5 above, all the respondents mentioned that abductions and thefts as major personal security risks that could occur (100%). This was followed by rape (93.4%), robberies (92.6%), breakings (86.8%), murders (86.0%) and lastly burglaries at 84.4%.

Besides, the respondents were asked to mention other security risks in addition to what was already listed by the researcher.

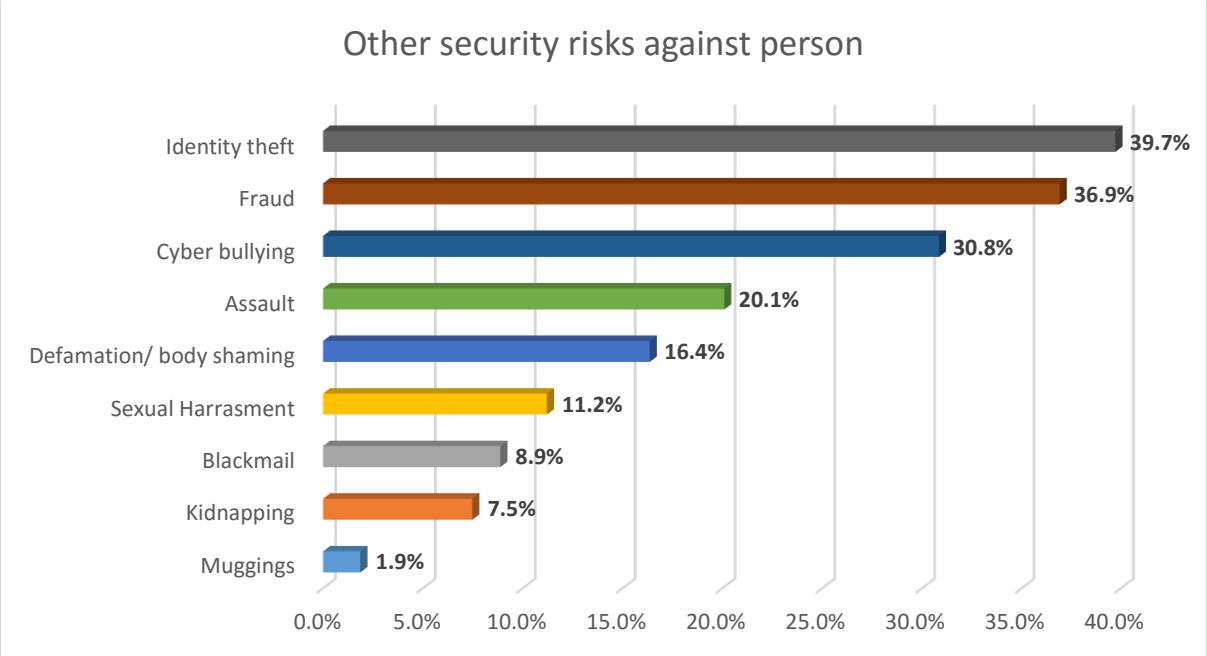

Figure 4.8: Other personal security risks

Based on Figure 4.8 above, other security risks that were mentioned by the respondents include identity theft (39.7%), fraud (36.9%), cyber bullying (30.8%), assault (20.1%), body shaming (16.4%), sexual harassment (11.2%), blackmail (8.9%), kidnapping (7.5%) and muggings (1.9%).

Common crimes

In addition, the study sought to establish the common crimes in the respondent's neighborhoods of Kawangware and Kilimani. Here, the respondents were asked to state the common crimes within their neighborhoods and this data was cross tabulated to compare the two areas within Dagoreti North Sub-County. Findings were as shown in Table 4.12 below.

Table 4.12: Common crimes

			Residence		*Total*
			Kawangware	**Kilimani**	
Common offenses	Abductions	Count	29	27	56
		% within Residence	51.8%	48.2%	
		% of Total	7.7%	7.1%	14.8%
	Break-ins	Count	24	48	72
		% within Residence	33.3%	66.7%	
		% of Total	6.3%	12.7%	19.0%
	Cyber bullying	Count	9	27	36
		% within Residence	25.0%	75.0%	
		% of Total	2.4%	7.1%	9.5%
	Identity theft	Count	5	45	50
		% within Residence	10.0%	90.0%	
		% of Total	1.3%	11.9%	13.2%
	Kidnapping	Count	2	24	26
		% within Residence	7.7%	92.3%	
		% of Total	0.5%	6.3%	6.9%
	Murders	Count	4	15	19
		% within Residence	21.1%	78.9%	
		% of Total	1.1%	4.0%	5.0%
	Rape	Count	11	33	44
		% within Residence	25.0%	75.0%	
		% of Total	2.9%	8.7%	11.6%
	Robberies	Count	65	31	96

Continuation of table 4.13: Common crimes

		% within Residence			
		% of Total	17.2%	8.2%	25.4%
	Sexual	Count	12	12	24
	Harassment	% within Residence	50.0%	50.0%	
		% of Total	3.2%	3.2%	6.3%
	Theft	Count	83	56	139
		% within Residence	59.7%	40.3%	
		% of Total	22.0%	14.8%	36.8%
	Blackmail	Count	9	0	9
		% within Residence	100.0%	0.0%	
		% of Total	2.4%	0.0%	2.4%
	Fraud	Count	9	19	28
		% within Residence	32.1%	67.9%	
		% of Total	2.4%	5.0%	7.4%
Total		Count	197	181	378
		% of Total	**52.1%**	**47.9%**	**100.0%**

Overall, based on the results on Table 4.12, the common offenses were occurring at a slightly higher rate of 52.1% in Kawangware than in Kilimani (47.9%). Over three quarters of the cases of cyber bulling as a common offense were experienced in Kilimani 75.0% than in Kawangware (25%). This was also the same case with rape (Kilimani 75.0%; Kawangware 25.0%), kidnapping (Kilimani 92.3%; Kawangware 7.7%), break ins (Kilimani 66.7%; Kawangware 33.3%), identity theft (Kilimani 90.0%; Kawangware 10.0%), murders (Kilimani 78.9%; Kawangware 21.1%), and fraud (Kilimani 67.9%; Kawangware 32.1%). Some of the common offences that occurred in Kawangware than in Kilimani include blackmail (Kawangware 100.0%), abductions (Kawangware 51.8%; Kilimani 48.2%), theft (Kawangware 59.7%; Kilimani 40.3%) and robberies (Kawangware 67.7%; Kilimani 40.3%). The results indicated

that sexual harassment took place at the same rate in the two areas (Kawangware 50.0%; Kilimani 50.0%).

Link between crime and use of social networking sites

The study also sought to identify the link between crime and the use of social networking sites. The respondents were asked if they thought there was any link between the offenses mentioned with information shared by the victims in their Social Networking user sites. The results were as illustrated in Figure 4.9 below.

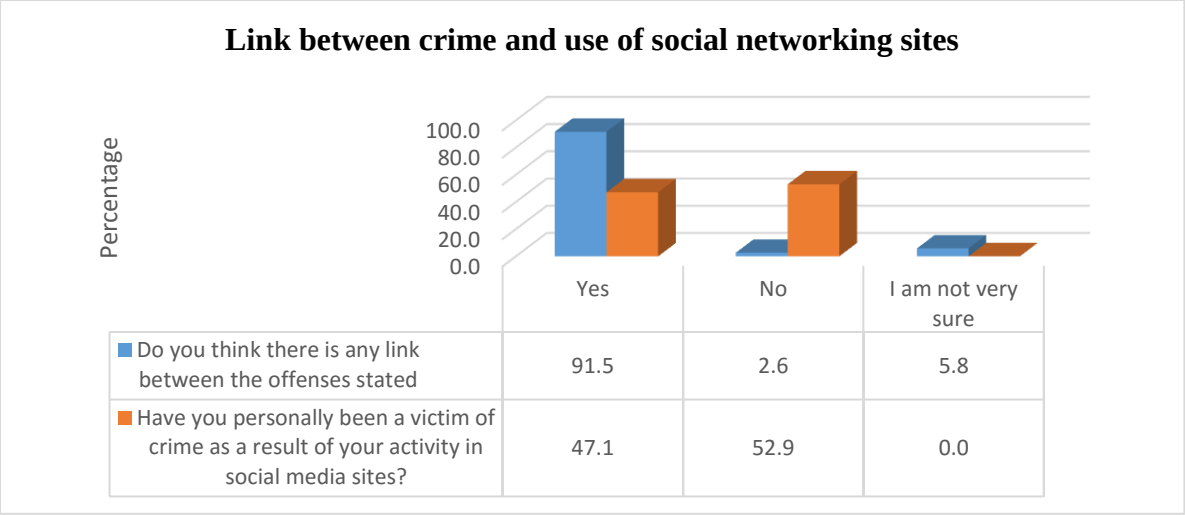

Figure 4.9: Link between crime and use of social networking sites

Based on Figure 4.9 above, the results indicate that a majority of the respondents (91.0%) agreed that indeed there was a link between crime and use of social networking sites while only a paltry 9.0% disagreed. When asked whether they had personally been victims of crime as a result of their activity in social media sites, nearly half of the respondents (47.0%) agreed while the rest (53.0%) disagreed.

Moreover, the study sought to explore whether there were any differences in opinion across various demographic characteristics of the respondents. Therefore, data on the whether the respondents had been victims of crime due to their activities in social media sites was cross-tabulated with the various socio-demographic characteristic. The results were as shown in Table 4.13 below.

Table 4.14: Whether respondents have been crime victims vs demographic characteristics

		Have been a victim of crime as a result of your activity in social media sites		χ^2*- Value*	*df*	*P-Value*
		Yes	No			
Gender	Male	68.6%	31.4%	87.511	1	0.000
	Female	20.2%	79.8%			
Age	18 - 30 years	49.6%	50.4%	66.97	3	0.000
	31 - 40 years	61.3%	38.7%			
	41 - 50 years		100.0%			
	51 - 60 years	40.9%	59.1%			
Level of	Secondary	0.0%	100.0%	11.982	1	0.001
education	Tertiary	48.8%	51.2%			
Employment	Unemployed	25.4%	74.6%	17.806	2	0.000
status	Self Employed	60.0%	40.0%			
	Formal employment	47.0%	53.0%			
Residence	Kawangware	53.8%	46.2%	7.45	1	0.006
	Kilimani	39.8%	60.2%			

Based on results in Table 4.13 above, all the various demographic characteristics reported divergent opinions on whether they had been victims of crime due to their activities in social media. In this regard, 68.6% of the male respondents reported to have been crime victims as a result of what they had posted in social media compared to 20.2% of their female counterparts who had fallen crime victims. With regards to age, quite a number of respondents had fallen victims of crime due to their activities in social media. For instance, 49.6% of respondents aged between 18-30 years, 61.3% of respondents between 31-40 years and 40.9% of those aged above 50 years reported to have been crime victims. On the other hand, none of the respondents between 41-50 years old had fallen victims of crime due to their social media activities.

With respect to education, none of the respondents who had at most secondary school education reported to have been victims of crime as a result of their activities on social media compared to 48.8% of the respondents with tertiary education who had been crime victims. Comparing the

different employment statuses, 25.4% of the unemployed, 60.0% of the self-employed and 47.0% of the formally employed respondents had been crime victims as a result of their activities on social media while 74.6% of the unemployed, 40.0% of the self-employed and 53.0% of the formally employed respondents respectively had not been crime victims due to social media activities. Finally, 53.8% of the respondents in Kawangware reported to have been crime victims compared to 39.8% of the respondents in Kilimani area. These differences were statistically significant at p-value < 0.05.

4.4.3 Risk mitigation measures to cushion social networking users

The third objective of the study sought to establish the risk mitigation measures geared to cushion social media users.

Table 4.14: Mitigation measures

	Yes (%)	***No (%)***
Never display details of personal or financial documents	100.0	0.0
Turn Off Automatic Login Features	100.0	0.0
Stop Posting of Location Updates	93.9	6.1
Stop Posting photo, date of birth, location, place of work	81.5	18.5
Use of Strong and Unique Passwords	96.6	3.4
Avoid Geo-Tagging Photos	93.9	6.1
Use of Protection Services such as Identity Guard and Life	96.0	4.0
Enabling Alerts of Unusual Activity in user accounts	96.6	3.4
Awareness talks at both Organizational and community levels	93.7	6.3

As evidenced on Table 4.14 above, all the respondents affirmed that they never displayed details of personal or financial documents and they also turned off automatic login features as part of the most common mitigation measures. Some of the other common mitigation measures as pointed out by the respondents include the use of strong and unique passwords and enabling alerts of unusual activity in the user accounts (96.6%), use of protection services such as identity guard and life (96.0%), avoiding geo-tagging photos and not posting of location updates (93.9%) as well awareness talks at both organizational and community levels (93.7%). The results also indicated that the least used mitigation measure was not posting of photo, date of birth, location and place of work.

Information from Key informants further revealed that in order to mitigate against security risks, relevant agencies such as Communication Authority of Kenya (CAK) can mitigate on this through appropriate data protection policies. The government through parliament should come up with a law to punish those who send threats and interfere with personal security especially on social media. More specifically, they should enact laws protecting e-consumers and watchdog over sites, and introduce more stringent legal framework to protecting social media users from such vices, while also making hacking a serious punishable crime. Also, there is need for the Communication Authority to develop their own superior site to detect fraudsters and enhance cyber security.

Another way these security risks can be mitigated against was said to be sensitization of users on the need to be aware that personal identifiable information shared on social media can be used against them by criminals. The users also need to be educated on the possible crimes they are likely to be exposed to when they disclose their personal information on social media. There is also a need to Educate the mass on the negative side of showcasing personal lifestyle on social media. Besides, it was suggested that there was need to sensitize people on how they can counter attack in the event these crimes happen and where to report such crimes. One of the informants stated,

> *"As stated above the best way is for the government to promote community awareness of this topic involving a simple effective program planned and implemented by professionals to the layman "mwananchi" at all levels".*

Moreover, it was suggested that the government should empower the ICT department to help them in bringing and updating systems that can help protects and campaign for safety to users. Further, the Key informants said that there was need to regulate internet access and above all, provide safer ways to connect to people. This regulation can be done by vetting of users as well as the information shared on social media, through proactive monitoring of suspect social media accounts, limiting access of social media to personal information, control access of information by secondary group, and by ensuring strict compliance of data law.

Another informant stated;

> *"In order to control the security threats as a result of using social media, there is need for the government to sensitize the public, sanitize social media by prosecuting the offenders quicker, enact the protection of digital information act, and ensure digital*

players have dedicated personnel to call for such issues e.g., Safaricom for hacking and deregistering of data".

4.5 Discussion

This section discusses the findings above in relation to other research studies conducted. The section is organized as per the objectives and include comparison with other studies. The study objectives included the identification of the features of online interaction in social networking user sites and their implication on personal security, identification of personal security risks associated with interaction on social networking user sites as well as establishment of the risk mitigation measures to cushion social networking users of Dagoretti North Constituency residents in Nairobi County, Kenya.

4.5.1 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 respondent's 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) reiterated 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, 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. Furthermore, they 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.

When it comes to the use of Pseudo names and credentials, one may pretend to be someone else and in the real sense he is not. This poses a threat as one may be exposed to criminals. The owners of these pseudo accounts engage in cyber bullying other social media users taking comfort in the hidden/false identity.

4.5.2 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. According to Kumar *et al.* (2016), by utilizing SNS, people open themselves to different sorts of dangers that have regular impact of breaking their privacy. Since SNS are quickly evolving and are facing a many-sided interaction with geo-economic and socio-cultural elements, it is important to constantly monitor how they develop, analyze how they work, and measure their potentialities.

The respondents 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 blackmail, 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. Wolak *et al.* (2006), conducting a similar study found out that, harassment among peers

has become unlimited thanks to the youth's access to the modern technologies. Bullying has shifted to a new territory, online (Li, 2006).

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 (Laudon *et al.,* 2010). While in many cases, this information is shared in posts, photos and profiles published on social media sites, the user's ability or inability to control access to this information posted on the social media sites has been a source of controversy. SNS continue to generate revenue with targeted advertising, based on personal information and this encourages registered users to provide as much information as possible. With the 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, and 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.

4.5.3 Risk Mitigation Measures to Cushion Social Networking Users

The third objective of the study sought to establish the risk mitigation measures geared to cushion social media users. All the respondents made it clear that that they had taken risk mitigation measures to cushion themselves and their social networking users. The findings suggest that most of the respondents had never displayed details of personal or financial documents and they also turned off automatic login features as part of the most common mitigation measures. These findings concur with the works of Irshad and Soomro (2018) who list several raft measures to cushion victims of online users that include; to never display details of personal or financial documents: They argued that this is something that criminals of identity theft are mostly looking for to steal identities. Therefore, they suggest 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 reiterates the importance of turning off automatic login in an effort to prevent those who illegally access the device do not view any personal information. Some of the other common mitigation measures as pointed out by the respondents 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 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.

When it comes to studies on the use of strong passwords, Drager (2011) recommended the Use of Strong and Unique Passwords; that are strong, secure and unique such as making them alphanumeric with special characters helps in keeping identity thieves at bay. The results also indicated that the least used mitigation measure was not posting of photo, date of birth, location and place of work as the main purposes of these sites are based social interactions. However, Myhre (2013) recommended 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. This can be done by going into the settings of Facebook, Instagram, LinkedIn, Twitter accounts and changing the preferences for your personal data.

CHAPTER FIVE
SUMMARY, CONCLUSIONS AND RECOMMENDATIONS

5.1 Introduction

This chapter looks into the summary of the study, conclusions based on the findings and recommendations.

5.2 Summary

The study sought to assess the vulnerability of social networking user sites and its implication on personal security of Dagoretti North Constituency residents in Nairobi County, Kenya. Guided by this broad objective, the study sought to identify the features of online interaction in social networking user sites and their implication on personal security, identify personal security risks associated with interaction on social networking user sites as well as to establish the risk mitigation measures to cushion social networking users in Dagoretti North Constituency in Nairobi County, Kenya. The study adopted a cross-sectional survey design. This was due to the need to have a comprehensive coverage of the phenomenon under study; to assess the vulnerability of social networking user sites and its implication on personal security of Dagoretti North Constituency residents in Nairobi County, Kenya.

Under the first objective, on the identification the features of online interaction in social networking user sites and their implication on personal security, the study revealed that Google+, Facebook and Instagram were the most used social networking sites while Friendster and Myspace were the least used sites. WhatsApp and Tiktok were the other popular and most recent sites to have a huge number of users across the world. There was a more frequent use of Facebook, Instagram, Google+ and Twitter with respondents using these sites on a daily basis. LinkedIn was used often as the respondents indicated that they used it at least once per week. The sites acquired the geographical coordinates of users, allowed the use of pseudo names and credentials, made it easy to find victims with just a few keystrokes, could allow replication of information and conceal originality, steal someone's credentials, ascertain those who might run across victim expressions in networked publics as well as allow being invisible audiences.

Under the second objective on the identification of personal security risks associated with interaction on social networking user sites, the study revealed that nearly all the respondents agreed that there was a relationship between social media use and the threat to personal security. Abductions and thefts were mentioned 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 blackmail, 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. Under the third objective on the establishment of the risk mitigation measures to cushion social networking users, the study revealed that the most of the respondents had never displayed details of personal or financial documents and they also turned off automatic login features as part of the most common mitigation measures. Some of the other common mitigation measures as pointed out by the respondents 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 awareness talks at both organizational and community levels.

5.3 Conclusions

This section covers conclusions of this study based on research findings. The conclusions are divided into two categories namely: theoretical conclusions; and, empirical conclusions.

5.3.1 Theoretical Conclusions

This study was guided by Protection motivation theory to understand online safety behaviors in the context of social media use and mitigate on resultant threats. The study assumed that using different social Media sites make users to experience a variety of online security threats that require them to enact safety precautions. In this study, PMT has been used as a powerful model to understand and predict the adoption of protective technologies, and one of the main theoretical foundations in the information security research field, which helps users avoid harm from a growing number of negative technologies by practicing healthier behaviors when dealing with security issues. As PMT theorizes, perceived rewards neutralize much of the effect of perceived severity and perceived vulnerability resulting in a lower threat assessment and hence a greater likelihood of engaging in the behavior. By underlining the two processes to predict and mediate protection motivation: threat appraisals and mitigation appraisals, this study shows that the exposure to personal security risks such as abductions, burglary, theft of identity, rape, murders, kidnapping, breakings and cyber bulling are a threat enough to the users of the SNS for them to put in place mitigation measures such as the use of strong passwords, turn off

locations, geo-tagging of photos, restraint in posting personal identifiable information and turning off automatic log in features amongst others in an effort to protect themselves.

5.3.2 Empirical Conclusions

The study sought to assess the vulnerability of social networking user sites and its implication on personal security of Dagoretti North Constituency residents in Nairobi County, Kenya. The study's first objective sought to identify the features of online interaction in social networking user sites and their implication on personal security. The study concludes that Google+, Facebook and Instagram are the most used social networking sites while Friendster and Myspace are the least used sites. The study further concludes that in the recent years, WhatsApp and Tiktok have emerged as the other popular sites adopted by users across the world. There appears to be a more frequent use of Facebook, Instagram, Google+ and Twitter as respondents are using these sites on a daily basis. LinkedIn is also used often as the respondents indicate that they used it at least once per week. The sites continue to acquire the geographical coordinates of users, allow the use of pseudo names and credentials, making it easy to find victims with just a few keystrokes, the sites further allow replication of information and concealing of originality.

The second objective of the study sought to identify personal security risks associated with interaction on social networking user sites in Dagoretti North Constituency residents in Nairobi County, Kenya. This objective concluded that there was a relationship between social media use and the threat to personal security. Abductions and thefts are the major personal security risks as well as rape, robberies, breakings, murders and burglaries. Among the two areas of study, Kawangware is the area with most of these cases when compared to Kilimani. Some of the most common offences in Kawangware include blackmail, abductions, theft and robberies. On the other hand, Kilimani has cyber bullying, rape, kidnapping, breakings, identity theft, murders and fraud as the most common offences. Sexual harassment is equally experienced in both areas.

The study's final objective was to establish the risk mitigation measures to cushion social networking users in Dagoretti North Constituency in Nairobi County, Kenya. The findings of this objective concluded that most of the respondents have never displayed details of personal or financial documents and they also turned off automatic login features as part of the most common mitigation measures. Some of the other common mitigation measures as concluded by the study findings 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 awareness talks at both organizational and community levels.

5.4 Recommendations

In order to address the personal security risks brought about by disclosure of personal identifiable information on social networking sites on the users, this study makes the following recommendations:

i. In the study identified features of all online interaction in social networking user sites and their implication on personal security. These features included the ability to; acquire the geographical coordinates of users, allow the use of pseudo names and credentials to conceal the identity of criminals, make it easy to find victims with just a few keystrokes, the sites further allow replication of information and concealing of originality. According to this study, all SNS were found to expose users to compromise personal security. Because of this study recommends, to the Government through ICT ministry; can generate policies that makes it mandatory to target hardening their privacy settings, and introduce security induction package may involve settings that can enable users to limit the amount of personal data that third-party applications can access. Through Policy, user education programmes should be entrenched and made mandatory in learning institutions. Awareness campaigns should also targeted Television and Radio Audiences. National Government Administrative Officers (The County Commissioners, Deputy County Commissioners, Chiefs and Assistant chiefs) may also support in sensitization campaigns to communities during public Baraza's.

ii. The second objective identified personal security risks associated with interaction on social networking user sites in Dagoretti North Constituency residents in Nairobi County, Kenya. Major risks include; abductions and thefts, rape, robberies, breakings, murders and burglaries. Based on this finding the study recommends that the states and its intelligence mechanisms have in addition to the conventional spying techniques enhance their information collection capabilities to online platforms such as the SNS. They ought to work in collaboration with users to ensure that SNS criminals are apprehended and their accounts permanently shut down. Inadvertent unsafe usage of SNS by individuals should be cut at the nib as it may lead to national security threats in future.

iii. The study established several risk mitigation measures to cushion social networking users in Dagoretti North Constituency in Nairobi County, Kenya that included identity guards and strong passwords with regard to email accounts but further recommended that by way of policy, the government should benchmark with developed countries for advanced preventive regulations measures against social networking vulnerability that cushion and protect SNS users.

5.5 Suggestions for Further Research

This study has established personal security risks brought about by disclosure of personal identifiable information shared by users on social networking sites at Dagoretti North Constituency residents in Nairobi County, Kenya. A similar study may be conducted somewhere else in similar contexts to compare findings with this study.

Secondly, how to limit access to personal information shared on SNS remains a grey area that needs further illumination by way of research. Given the degree of vulnerability to personal insecurity caused by its various online features, an urgent research should be carried out to establish any possibility of access to government security information that may be used by government enemy forces to the detriment of national security.

REFERENCES

Aday, S., Henry F., Marc L., & John, S. (2010). Blogs and bullets. *New Media in Contentious Politics. Peaceworks*, no. 65 (2010).

Albrechtslund, A. (2008). *Online social networking as participatory surveillance*. *First Monday, 13*(3). https://doi.org/10.5210/fm.v13i3.2142

Al-Daghir, M. M. A. (2013). The usage of media professionals to social media networks and perverted rumors, an applied study on the communicator in media institutions in Saudi Arabia. *Journal of the Faculty of Arts, the University of Zaqaziq, 64*(6), 542-552.

Boyd, D. (2007). Why youth (heart) social network sites: The role of networked publics in teenage social life. In *Youth, identity, and digital media* (Buckingham, D. Ed.). MIT Press.

Boyd, D., & Ellison, B. (2007). *Social network sites: Definition, history, and scholarship*. Michigan State University.

Boyd, D., & Ellison, N. B. (2008). Social network sites: Definition, history, and scholarship. *Journal of Computer-Mediated Communication, 13*(1), 210-230.

Byrne, D. N. (2008). Public discourse, community concerns, and civic engagement: Exploring black social networking traditions on blackplanet.com. *Journal of Computer-Mediated Communication, 13*(1), 319-340.

BITS (2011). Social media risks and mitigation: A division of the financial services round table, Pennysylvania. Retrieved on January 10, 2019, from https://www.nist.gov/system/files/documents/itl/BITS-Malware-Report-Jun2011.pdf

Black, S., Stone, D., & Johnson, A. (2014). Use of social networking websites on applicants'privacy. *Employee Responsibilities and Rights Journal, 27*(2), 115-159.

Chennamaneni, A., & Taneja, A. (2015). *Communication privacy management and self-disclosure on social media - A Case of Facebook*, 1–11.

Charnigo, L., & Barnett-Ellis, P. (2007). Checking out facebook.com: The impact of a digital trend on academic libraries. *Information Technology & Libraries, 26*(1), 23-34.

Choi, J. H. (2006). Living in Cyworld: Contextualising Cy-Ties in South Korea. In Bruns, A., & Jacobs, J. (Eds.), *Uses of blogs* (Vol. 7, pp. 173–186). Peter Lang.

Chipurici, C. (2016). *How to prevent identity theft.* Retrieved on January 10, 2019, from https://heimdalsecurity.com/blog/how-to-prevent-identity-theft-20-steps/.

Drager, D. (2011). Ways to prevent identity theft. Retrieved on January 10, 2019, from http://www.makeuseof.com/tag/9ways-prevent-identity-theft-online-activities/.

Experian, T. (2010). "Facebook fraud: Identity theft through social networking," Retrieved on March 12, 2018, from https://www.protectmyid.com/images/education_center/pdf/050TypesofFraud/7_types%20of%20fraud_social%20networking.pdf.

Elsevier, C. (2016). "Identity theft rises sharply as fraudsters target social media." *Computer Fraud & Security, 20*(7), 432-433.

FERF, & Thorton, G. (2011). *Social media and its associated risks*. Danvers.

Gross, R., & Acquisti, A. (2006). Imagined communities: Awareness, information sharing, and privacy on the facebook. In Danezis, G., & Golle, P. (Eds.) *Privacy enhancing technologies* (Vol. 4258, pp. 36-58). *PET 2006.* http://dx.doi.org/10.1007/11957454_3

Hargittai, E. (2008). Whose pace? Differences among users and non-users of social network sites. *Journal of Computer-Mediated Communication, 13*(1), 276-297.

Humphreys, L. (2008). Mobile social networks and social practice: A case study of Dodgeball. *Journal of Computer-Mediated Communication, 13*(1), 341-360.

Hoelscher, P (2017). Phishing Attacks. Retrieved on February 10, 2017, from http://resources.infosecinstitute.com/ category/enterprise/phishing/the-phishing-landscape/phishing-attacks-bydemographic/socialnetworks/#gref.

Kandikanti, P. (2017). *Investigation on security issues and features in social media sites (facebook, twitter & google+).* Governors State University.

Kim, K., & Yun, H. (2008). Cying for me, cying for us: Relational dialectics in a

Korean social network site. *Journal of Computer-Mediated Communication, 13*(1), 298-318.

Knorr-Cetina, K. (1997). Sociality with objects: Social relations in postsocial knowledge societies". *Theory, Culture, and Society, 14*(4), 1-30.

Lampe, C. A., Ellison, N., & Steinfield, C. (2007). A familiar face(book): Profile elements as signals in an online social network. In Proceedings of the SIGCHI conference on human factors in computing systems (pagg. 435-444). ACM. Retrieved on April 10, 2020, from http://portal.acm.org/citation.cfm?id=1240695.

Lange, P. G. (2008). Publicly private and privately public: Social networking on YouTube. *Journal of Computer-Mediated Communication, 13*(1), 361-380.

Liu, H., Maes, P., & Davenport, G. (2006). Unraveling the taste fabric of social networks. *International Journal on Semantic Web & Information Systems, 2*(1), 42-71.

Liu, H. (2008). Social network profiles as taste performances. *Journal of Computer- Mediated Communication, 13*(1), 252-275.

Liu, Y., & Ying, X. (2010). *A review of social network sites: Definition, experience and applications. The conference on web based business management.* Pearson.

Lippa, R. A. (1994). *Introduction to social psychology*. Wadsworth.

Mali, J. (2013). Identity theft through social networking. Retrieved on January 14, 2018, from http://www.lifehack.org/articles/technology/identity-theft-through-social-networking-lessons-take-now.html.

Milgram, S. (1967). The small world problem. *Psychology Today*.

Myhre, J. (2013). Social media security. Retrieved on January 11, 2019, from http://www.businessnewsdaily.com/ 4194social-media-security-tips.html.

Preibusch, S., Hoser, B., Gürses, S., & Berendt, B. (2007). Ubiquitous social networks: Opportunities and challenges for privacy-aware user modelling, DIW discussion papers, No. 698, Deutsches Institut für Wirtschaftsforschung (DIW). http://hdl.handle.net/10419/18430

Pattinson, M., & Anderson, G. (2007). How well are information risks being communicated to your computer end-users? Retrieved on January 10, 2019, from www.emeraldinsight.com/0968-5227.htm

Rohani, V., & Hock, S. (2009). On social network web sites: Definition, features, architectures and analysis tools. *Journal of Advances in Computer Research*, 1, 3-11.

Sarah, L., & Allee, M. (2016). Americans willing to give up privacy online for convenience. *VOCATIV*. Retrieved on January 10, 2019, from http://www.vocativ.com/271029/ pew-surveydigital-privacy-online/

Socialbakers (2013). Social media analytics: Uncovered Socialbakers. Retrieved on January 10, 2019, from https://www.socialbakers.com/blog/social-media-analytics-uncovered

Steinfield, J. (2007). Ways to avoid scams-when-using-social-media. Retrieved on January 18, 2019, from https://www.inc.com/joseph-steinberg/8-ways-to-avoid-scams-when-using-social-media.html

Stutzman, F. (2006). An evaluation of identity-sharing behavior in social network communities. *International Digital and Media Arts Journal, 3*(1), 561-571.

Skog, D. (2005). Social interaction in virtual communities: the significance of technology. *International Journal of Web Based Communities, 1*(4), 464-474.

Spertus, E., Sahami, M., & Buyukkokten, O. (2005). Evaluating similarity measures: A large-scale study in the Orkut social network. In *Proceedings of the eleventh ACM SIGKDD international conference on knowledge discovery in data mining*. ACM

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

Vander Veer, E. A. (2008). *Facebook: The missing manual*. Pogue Press.

Zhao, J., Binns, R., Kleek, M. V., & Shadbolt, N. (2016). Privacy languages: Are we there yet to enable user controls? Expression of privacy preferences, 799–806. http://dx.doi.org/10.1145/2872518.2890590

APPENDICES

Appendix I: Letter of Introduction

MOHAMED ABDUL M'MAKA
EGERTON UNIVERSITY
BOX 536
NJORO –KENYA

Dear Respondent,

RE: DATA COLLECTION

I am a student of Egerton University pursuing Master of Arts Degree in Security Management. I am currently conducting a research entitled "Assessing the vulnerability of social networking user sites and its implication on personal security of Dagoreti North Constituency residents in Nairobi County, Kenya.

I will highly appreciate if you participate in this study and assist me by responding to the questions that will follow. Your response will be treated with utmost confidentiality.

Thank You.

Yours Faithfully,

MOHAMED ABDUL M'MAKA

Appendix II: Questionnaires to the Main Respondents

Kindly fill the questionnaire as appropriately as possible. Be assured that the information you give

will be treated with utmost confidentiality and will be used only for research purpose.

SECTION A: BACKGROUND INFORMATION

1. Gender:

Gender	Male	Female

2. Age (years): ☐

3. Level of education: What is your level education (Tick where appropriate)

No formal Education	Primary	Secondary	Tertiary

4. Employment status

Self-employed ☐ Formal employment ☐

5. Residence ……

SECTION B: COMMON FEATURES OF SOCIAL NETWORKING USER SITES THAT CAN POTENSIALY PREDISPOSE USERS TO INSECURITY

1A. The following statements describe aspects of social Networking user sites. For each statement indicate your assessment by ticking in the box on the ones that you frequently visit either; 2=Yes or 1=No

No	Item	Yes	No
1A,1	Twitter		
1A,2	Facebook		
1A,3	Linkedin		
1A,4	Instagram		
1A,5	Google+,		
1A,6	Friendster		
1A,7	MySpace		

1B,8 Any other that was left out in 1A above? List them down

.....

.....

.....

.....

1.C The following statements describe aspects of social Networking user sites. For each statement indicate your assessment by ticking in appropriate box either; 2=Yes or 1=No

No	Item	Yes	No
1C,1	Inability to acquire the geographical coordinates of users		
1C,2	Use of Pseudo names and credentials		
1C,3	Finding victims is just a matter of keystrokes		
1C,4	Replicability of information and ability to conceal originality		
1C,5	Difficulty to distinguish “originality” from the “copy.”;		
1C,6	Easy to steal someone’s credentials		
1C,7	Invisible audiences		
1C,8	Impossibility to ascertain all those who might run across victim expressions in networked publics.		

2.0 What security implication does the features above have on the users

Inability to acquire the geographical coordinates of users

.....

.....

.....

.....

2.1 Inability to acquire the geographical coordinates of users

.....

.....

.....

.....

2.2 Use of Pseudo names and credentials

.....

.....

.....

.....

.....

2.3 Finding victims is just a matter of keystrokes

.....

.....

.....

.....

.....

2.4 Replicability of information and ability to conceal originality

.....

.....

.....

.....

.....

2.5 Difficulty to distinguish “originality” from the “copy.”;

.....

.....

.....

.....

.....

2.6 Easy to steal someone’s credentials

.....

.....

.....

.....

.....

2.7 Invisible audiences

.....

.....

.....

.....

.....

2.8 Impossibility to ascertain all those who might run across victim expressions in networked publics.

.....

.....

.....

.....

.....

SECTION C: PERSONAL SECURITY RISKS ASSOCIATED WITH INTERACTION ON SOCIAL NETWORKING USER SITES IN DAGORETI NORTH CONSTITUENCY.

3A The following statements describe the type of personal security risks that can occur as a result of information posted in social Networking user sites. For each statement indicate your assessment by ticking in appropriate box either; 2=Yes or 1=No

No	Item	Yes	No
3A,1	Robberies		
3A,2	Burglaries		
3A,3	Breakings		
3A,4	Murders		
3A,5	Abductions		
3A,6	Thefts		

3A,7	Rape		

3B,1 Is there anything crime against person that was left out in 3A above? Explain

.....

.....

.....

.....

3B, 2. Which offenses are very common in this area?

.....

.....

.....

.....

3B, 3. Do you think there is any link between the offenses stated above with information shared by the victims in their Social Networking user sites? Explain

.....

.....

.....

.....

SECTION D: RISK MITIGATION MEASURES TO CUSHION SOCIAL NETWORKING USERS

4A. The following statements describe aspects of the Risk Mitigation Measures to cushion victim's communication in their Social Networking user sites. For each statement indicate your assessment by ticking in appropriate box either; 2=Yes or 1=No

No	Item	Yes	No
4A1	Never display details of personal or financial documents		
4A,2	Turn Off Automatic Login Features		
4A,3	Stop Posting of Location Updates		
4A,4	photo, date of birth, location, place of work		
4A,5	Use of Strong and Unique Passwords		
4A,6	Avoid Geo-Tagging Photos		
4A,7	Use of Protection Services such as Identity Guard and Life		

4A,8	Enabling Alerts of Unusual Activity in user accounts		
4A,9	Awareness talks at both Organizational and community levels		

4B, 1 Is there anything else that you think was forgotten?

Thank you

Appendix III: Key Informants Interview Guide

1. How does the following Features of Online Social Networking user sites affect their personal security?

a) Inability to acquire the geographical coordinates of users

.....

.....

..

.....

..

(b) Use of Pseudo names and credentials of attackers

.....

.....

..

.....

.. ..

(c) Finding victims is just a matter of keystrokes

.....

.....

..

.....

..

.....

..

(d) Replicability of information and ability to conceal originality

.....

.....

..

.....

..

.....

..

(e) Difficulty to distinguish “originality” from the “copy.”

.....

.....

..

.....

.

.....

..

(f) Easy to steal someone’s credentials

.....

.....

..

(g) Invisible audiences

.....

.....

..

.....

..

.....

..

(h) Impossibility to ascertain all those who might run across victim expressions in networked publics.

.....

.....

..

.....

..

.....

..

2. What is the link between Crimes committed against victims and their families in Dagoreti North Constituency residents in Nairobi County, Kenya and their interactions on social networking user sites?

.....
..

.....
..

.....
..

3. What are Personal Level Mitigation Measures that can be used to cushion victims and their families in Dagoreti North Constituency, against insecurity that stem from their interactions in social networking user sites?

.....
..

.....
..

.....
..

.....
..

4. What are Community Level Mitigation Measures that can be used to cushion victims and their families in Dagoreti North Constituency, against insecurity that stem from their interactions in social networking user sites

.....
..

.....
..

.....
..

Appendix IV: Letter of Introduction from Graduate School

EGERTON UNIVERSITY
Tel: Pilot: 254-51-2217620
254-51-2217877
254-51-2217631
Dir.line/Fax: 254-51-2217847
Cell Phone
P.O. Box 536 - 20115
Egerton, Njoro, Kenya
Email: bpgs@egerton.ac.ke
www.egerton.ac.ke

OFFICE OF THE DIRECTOR GRADUATE SCHOOL

Ref: AM21/0217/12 Date: 10th June, 2021

The Director General
National Commission for Science Technology and Innovation,
P. O. Box 30623-00100
NAIROBI.

Dear Sir,

RE: REQUEST FOR RESEARCH PERMIT – MR. MOHAMED ABDUL M'MAKA REG. NO. AM21/0217/12

This is to introduce and confirm to you that the above named student is in the Department of Peace, Security & Social Studies, Faculty of Arts and Social Sciences, Egerton University.

He is a bona-fide registered M.A. student in this University. His research topic is **"Social Networking User Sites and Their Implication on Personal Security of Dagoreti North Constituency Residents in Nairobi County, Kenya".**

He is at the stage of collecting field data. Please issue him with a research permit to enable him undertake the studies.

Your kind assistance to him will be highly appreciated.

Yours faithfully,

14 JUN 2021

Prof. Nzula Kitaka
DIRECTOR, BOARD OF POSTGRADUATE STUDIES

NK/en

"Transforming Lives Through Quality Education"

Appendix V: Nacosti Permit

REPUBLIC OF KENYA

NATIONAL COMMISSION FOR
SCIENCE,TECHNOLOGY & INNOVATION

Ref No: **418905**

Date of Issue: **22/June/2021**

RESEARCH LICENSE

This is to Certify that Mr.. Mohamed Abdul Mmaka of Egerton University, has been licensed to conduct research in Nairobi on the topic: SOCIAL NETWORKING USER SITES AND THEIR IMPLICATION ON PERSONAL SECURITY OF DAGORETI NORTH CONSTITUENCY RESIDENTS IN NAIROBI COUNTY, KENYA for the period ending : 22/June/2022.

License No: **NACOSTI/P/21/11319**

418905

Applicant Identification Number

Director General
NATIONAL COMMISSION FOR
SCIENCE,TECHNOLOGY &
INNOVATION

Verification QR Code

NOTE: This is a computer generated License. To verify the authenticity of this document, Scan the QR Code using QR scanner application.

Appendix VI: Published Paper Abstract

RESEARCH ARTICLE

European Journal of Humanities and Social Sciences
www.ej-social.org

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

M. A. M'maka, P. Mwaeke, 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

Published Online: December 22, 2021
ISSN: 2736-5522
DOI: 10.24018/ejsocial.2021.1.6.183

M. A. M'maka*
Department of Peace Security
Social Sciences, Egerton University, Kenya.
(mohamedmmaka@gmail.com)
P. Mwaeke
Department of Peace Security
Social Sciences, Egerton University, Kenya.
(pamol.mwaeke@egerton.ac.ke)
E. Bor
Department of Peace Security
Social Sciences, Egerton University, Kenya.
(erick.bor@egerton.ac.ke)

**Corresponding Author*

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