SOCIAL MEDIA INFLUENCE ON PERSONAL SECURITY AMONG THE YOUTH IN NAIROBI CITY COUNTY, KENYA

SOITA NAFULA SALLY

C159/CTY/PT/38456/2016

A RESEARCH PROJECT SUBMITTED IN PARTIAL FULFILMENT FOR THE AWARD OF DEGREE OF MASTER OF ARTS IN SECURITY MANAGEMENT AND POLICE STUDIES IN THE SCHOOL OF SECURITY, DIPLOMACY AND PEACE STUDIES OF KENYATTA UNIVERSITY.

APRIL, 2022

DECLARATION

The work reported in this project is my original work and has not been submitted to any other university for the award of a degree. All sources of information have been acknowledged by way of references.

Signature …… Date ……

SOITA NAFULA SALLY

C159/CTY/PT/38456/2016

This research project has been submitted with my approval as University Supervisor.

Signature …… Date ……

DR. HARRISON NJOROGE

KENYATTA UNIVERSITY

DEDICATION

This research project is dedicated to my family and friends for the continued support since I began this journey, special thanks to God for enabling me come this far, my parents Geoffrey and Praxides Soita, siblings Sylvia, Shilla, Sharon and Samuel.

AKNOWLEDGEMENT

I thank my supervisor for being instrumental during this journey despite corona virus pandemic, am grateful for the support of all the lecturers in Kenyatta University and specifically Department of Security and Correction Science.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

DEFINITION OF TERMS

Cyber bullying:	Harassment on cyber space
Cyber stalking:	Refers to the use of social media to frighten people
Cybercrime:	Refers to crimes that target a computer or network
Hacking:	Refers to unauthorised access into a computer or a computer network.
Identity theft:	Refers to the use of a different identity to conceal the original
Internet:	Global connected networks that enable communication through various media
Malware:	Refers to malicious programs aimed at destroying a computer
Online romance scam:	Refers to online relationships that are meant to dupe a victim as a way of soliciting individual interests
Personal Security:	Refers to an individual being free from crime or violence on social media
Social media crimes:	Refers to crimes committed on social media platforms
Social media:	Global communication sites that require computer network also referred to as social networking sites or internet technologies
Youth:	Refers to group of people aged between 18-35 years according to Kenyan Constitution

LIST OF ABBREVIATIONS AND ACRONYMS

CAK	Communication Authority of Kenya
Email	Electronic mail
NACOSTI	National Commission for Science, Technology and information
NW3C	National White Collar Crime Centre
PCAK	Professional Criminologists Association of Kenya
SDG's	Sustainable Development Goals
SPSS	Statistical Packages for Social Sciences
US	United States

ABSTRACT

Use of social media has become a very important aspect of modern life. Growing use of social media has been associated with positive and negative outcomes such as considerable personal security risks. This study examined social media influence on personal security among youth in Nairobi County. The objectives of the study were to determine the forms of social media, crimes, to examine crimes that result from social media use among the youths to analyse the influence of social media on personal security and to identify challenges facing the prosecution of social media crimes to identify challenges facing law enforcement in investigating, prosecuting and preventing social media crimes in relation to personal security among the youths in Nairobi County. The study was guided by victim precipitation theory and space transition theory. The target population were members of Professional Criminologists Association of Kenya, PCAK. Purposive sampling was used to select 155 youth respondents from a population of 15000 youths and 145 law enforcement interviewees drawn from 2,000 law enforcement officers in PCAK in Nairobi County. Piloting of questionnaire were disseminated among 30 PCAK youths Nakuru chapter. The research instruments were verified by the supervisor for content validity. Statistical Packages for Social Sciences, SPSS software was used in data entry and descriptive statistics was used to analyse the data. Qualitative data was analyzed using content analysis, coding, classification and text inferencing. This study was significant to academic research, criminal justice practitioners and the private sector to assist in goal formulation and achievement of cyber security. Results of this research showed that forms of social media that youth mostly prefer is WhatsApp over other social media platforms. The most preferred social media platforms by both gender was found to be WhatsApp and Twitter. The findings of this research showed that about 84% of youth respondents in Nairobi City County had opinion that Facebook was most insecure. Further, about 52% of the youth respondents confirmed that they had been victims. Tracking offenders , lack of technological capacity and legal challenges. It was recommended that future research can focus on the issue of spatial dispersion of social media security influences on in Nairobi City County. Such dispersions should be based on real social media crime incidences by type time and location to give insights on how policing can be enhanced in response to such dispersion and temporal diffusion of such crimes especially on mobile platforms.

CHAPTER ONE

INTRODUCTION AND BACKGROUND

1.1 Introduction

This chapter comprises of the background to the study, the problem statement, research objectives, research questions, significance and scope of the study.

1.2 Background to the study

Social media can be defined as digital platforms that involve interaction among several users by sending messages or calling in a simpler and faster way that only requires internet connection and a smart phone or a computer (Jeesmitha & Com, 2019). In the past communication was slower as it was done through letters, telephone calls or newsletters .Improvement of technology has led to improved communication globally, social media involves interaction through creation of accounts where users exchange ideas ,goals and keep track of each other (Akakandelwa & Walubita, 2017). Early form of social media dates back to 1997 referred to as Six degrees founded by Andrew Weinreich based in New York, it had millions of users who were able to create online profiles interact with others however, it was limited by internet connectivity which was not common among people at that time (Jeesmitha & Com, 2019). In early 2000s other social networking sites such as LinkedIn and Myspace gained popularity. Facebook and Twitter which are most popular platforms had already spread to most countries by 2006. Today, there are many social media sites depending on individual preference (Jeesmitha & Com, 2019).

The concept of personal security was derived from Human security that narrows down the definition of traditional security which was state centred to people centred. It was first introduced in 1994 by Human Development Report that is traced back in President Franklin D.

Roosevelt speech in 1941 advocated on a world founded on freedom. Human security can be classified into economic security, health security, personal security, political security, food security, environmental security and community security (Security & Integration, 2020). Personal security also referred to as individual security advocates for freedom of expression, freedom of speech, expression, fear, want and freedom of worship. It gives the individual a greater sense of availability of threat and implementing various solutions to eliminate them (Gierszewski, 2017).

Personal security protects the individual from violence either from state or nonstate actors, exploitative adults and domestic abuse. It states that the common source of anxiety for most people is crime especially violent crime. Personal security has been classified into three groups according to the type of threat first, threat from internal or external factors including armed conflict, secondly threat from diverse kind of crimes from state or others then finally threat to own self such as drugs and suicide(Gasper & Gomez, 2015). The first threat to personal security is from external factors such as armed conflicts. Social media has been used in Arab countries such as Egypt and Tunisia to spread armed conflicts ideologies by recruiting new members, shaping their thoughts and organizing protestors (Cibra, 2017).

Threats to personal security result from suicide, drug and substance abuse which have been communicated on social media by individual postings have been witnessed online on alcohol and substance abuse in social places hence influencing other people(Luxton et al., 2012). A person battling with depression posted online how life has been unfair and how he saw no need to go on living, while most friends gave comments to encourage him not to give up, his mind was already made up only to be found dead in his house. Close relatives and friends are likely not to take the communication seriously when the matter is serious, a case is reported of a university student who committed suicide after a friend leaked his private video on twitter (Intahchomphoo, 2018)

A great deal of studies have addressed social media influence on security at global, regional and local levels. At global level, studies have focused on cross-border persective involving multiple countries in different continents (Asongu et al., 2019; Ghai et al., 2022; Karim & Al-Rawi, 2018). Such studies have generally concluded that social media use influence personal security of individuals, including the youth. In different Countries, such as U.S, Korea, Israel, Canada and Sweden have about two thirds of adults using social media (Gottfried & Shearer, 2019). Developing countries in Asia, Middle East and Africa for example Jordan, Phillipines, Lebanon, Indonesia and Tunisia there is widespread social media usage and greatly influences on personal security of youth (Center, 2018). All over the world, social media provides communication among young people through chatting they are able to connect with friends, video calls have also provided wider avenues for interaction among young people and has also been an avenue for security breaches (Akakandelwa & Walubita, 2017). Availability of bundles using smartphones and Wi-Fi connections have made social media communication easier (Hruska & Maresova, 2020). Twitter and Facebook have been ranked as the social media sites with the highest number of people, (Chege, 2019). The second threat to personal security on cyber space is crime, risks on Social media are widely discussed and commonly feature among several countries including the access of personal data by engaging the users on leading questions. Cyber criminals target victims in social media sites such as Facebook, twitter and LinkedIn (Gachau, 2018). Facebook scam include photo notification scam that redirects to a different source, Facebook chats also promote spread of malware and phishing that solicit important information from unsuspecting users. On Twitter, attackers use attractive tweets to gain the attention of the followers such as free vouchers (Ackerman & Schutte, 2015). Such studies focus on different types of security threats and risks across different social media platforms but fail to substantively focus on personal security. The studies treat security generally.

In Europe studies have shown that youths spend more time on social networking sites for educative purposes such as sharing and communicating among themselves and this has made them vulnerable to social media crimes (Bradshaw, Neudert, & Howard, 2018). Various European learning institutions also avail important information through blogs or YouTube channels teachers are able to post about class activities and various events on social media to keep students updated (Patel & Prajapati, 2018). Online businesses are promoted on social media by focusing on customers likes and dislikes also increase market insight beyond the rivals (Hruska & Maresova, 2020). European countries have made an efforts to keep up with the latest Internet developments such as social media security issues and associated digital practices among the youth with the goal of establishing secure Europe (Costa & Murphy, 2019). Whereas the studies in Europe focus on youth as major users of social media, the studies fail to identify aspects of personal security that are influenced and treat security without going into specifics. Therefore, the relationship between each form of social media and personal security has not been established even in Europe.

In the North and South America, main forms of social media commonly used include YouTube and Face book with 68% of adults using Facebook, however young adults (18-24years) frequently use Instagram and Snap chat (Richins, 2015). In South American countries, the trend varies among countries depending on technology. Research has found out that social media is an increasingly prevalent fixture for youth in the USA with more than 90 percent of teenagers using it daily (Byrne, Vessey, & Pfeifer, 2018). Though social media has provided many positive opportunities for youths, it has also become a major platform for cybercrime and violent extremism (Alava, Frau-Meigs, & Hassan, 2017; Byrne, Vessey, & Pfeifer, 2018). Victims of social media crimes vary according to crime and the age group, economic factors play a crucial role in cyber stalking, cyber stalkers have intentional motives towards their victims as reported by National White Collar Crime Centre (NW3C) female victims have been

found to be targets of cyber stalking. In the USA, however ,a survey showed that males constituted of majority of cyber stalking victims (Soomro & Hussain, 2019) .Single individuals are likely to experience cyber bullying than the married counterparts this may be attributed to loneliness and search for a life partner especially when they read about success stories of people who met in social platforms (Stone, 2020). Creation of accounts on social media requires personal information that may easily put one as a suitable target to cyber criminals. Sharing of photographs is common across social media sites, this is even more risky as the smartphone used contains the metadata that includes the camera details and location of the user which the photograph was taken putting the user at risk (Zappavigna, 2016). A study shows that most users will take pictures at places they mostly frequent such as homes, work places or places they like to visit (Ghazinour & Ponchak, 2017).

In the Middle East, social media has continued to be popular among Arab youth (Radcliffe & Bruni, 2019). There have also been increasing security challenges as a result of online freedom of expression in many parts of the Middle East region (Tufekci, 2018). Countries such as Saudi Arabia and United Arab Emirates are social media powerhouses, and are big national markets for Snapchat and YouTube in the world (Radcliffe & Bruni, 2019). Social media use among the youth in these countries has met with some pushback where strict regulations have been developed in UAE, and major threats in Iraq (AlNajjar, 2019). There are now concerns about rise of fake news on social media, threats to personal security and the role that social networks are playing in terrorism and Yemen's civil war (Al-Shami, 2021; Ruggiero, 2019). Social media has been used in the search for potential job seekers among several companies in the Middle East, however the applicants may be targeted by criminals with fake job recruitments (Al-Amin et al., 2019). Most organizations have social media pages and email addresses that can be manipulated by cyber criminals to get personal information from victims curriculum vitae and also demand for money before interviews. Most professionals globally have social media

handles, job seekers interact with the employers as soon as they get advertisements for specific job descriptions, however the invasion of privacy from cyber criminals may pose a challenge to the candidates (Tikhonov & Konovalova, 2020)

In Africa, young people use social media for entertainment, social interaction and research. In South Africa most of the youths spend time chatting, uploading content, downloading video games and getting news updates, and sharing knowledge. Facebook tops the list then YouTube and twitter among social media users in South Africa (Shava & Chinyamurindi, 2018). In Nigeria, social media has been used by terror groups such as Boko Haram to perpetrate insecurity (Omede & Alebiosu, 2020). Nigerian security agencies monitor social media to be able to sieve out and react to all anti-government, anti-military and anti-security communications on social media (Ogunlana, 2019; Omede & Alebiosu, 2020). It has also been established in literature that social media has been used to target victims for ritualism and sacrifices in West African countries as well as parts of East Africa (Olofinbiyi, 2021).

In Kenya, according to the Communications Authority of Kenya (CAK) there are about 40.4 million mobile phone subscribers in Kenya, the trend keeps on increasing commonly downloaded applications are Facebook, branch, Facebook messenger, WhatsApp, Tala, True caller and Opera mini. Majority of the users are on WhatsApp at 12 million and the least being Snap chat at 0.25 million (Bake, 2018). In Kenya, Al-Shabaab and al-Qaeda Muslim jihadists use Facebook, twitter and YouTube to spread news to their sympathisers and causing fear to the entire population by posting images of successful attacks this in turn fuels hatred social media provides direct communication between the terrorists and interested parties (Project et al., 2018). During the post-election violence in Kenya, social media was used to spread propaganda, regrouping of people and provide updates about the crisis while fuelling ethnic hatred (Kižina, 2015). Previous research on influence of social media use in Africa and Kenya has largely focused general security but have not specifically addressed personal security

(Munyua, 2013; Kwanya, Kogos, Kibe, Ogolla, & Onsare, 2021; Okuku, Renaud, & Valeriano, 2015).

1.3 Statement of the Problem

In Kenya, offenses against individuals were found to constitute the main type of crime reported to the police in 2019 where there were 27.2 thousand cases. Reported cybercrimes in Kenya was about 140 million in 2020 and has continued to increase (Faria, 2021). According to Vidja (2021), Kenya is facing a possible increase in cybercrime in 2021, with malware attacks were the highest at 46 million, web application attacks at 7.8 million and 2.2 million distributed denial of service (DDOS) (Vidija, 2021). Cyber criminals in Kenya have recently been targeting enterprises and individuals who lose millions of shillings to cyberattacks and sometimes lose property and life as hackers target those with little or no defences on their digital systems (Sunday, 2021). These have been correlated with rise in child theft, hijacking, kidnapping, scams, cyberfraud, cyberbullying and other crimes against persons mainly perpetrated based on social media.

Social media users have increased over the years this is due to a wide range of social media forms as social networks such as Facebook, Twitter, LinkedIn and WhatsApp; media sharing networks e.g. Instagram, YouTube and Emails; discussion forums e.g. Reddit, Quora and blogging and publishing networks. Social media use among youth has been associated with influences on personal security. Factors such as victim predisposition to cyber-attacks, presence of vulnerabilities in network, lack of specific legal framework to deal with cybercrime and inadequate capacity of law enforcement to deal with online crimes has led to cases of breach to personal security.

Previous research on influence of social media use in Kenya has largely focused general security but have not specifically addressed personal security (Munyua, 2013; Kwanya, Kogos,

Kibe, Ogolla, & Onsare, 2021; Okuku, Renaud, & Valeriano, 2015). Whereas there has been focus on various devices such as mobile phones and social media crimes perpetrated in them, there has not been substantive focus on personal security. The problem is that relationship between each form of social media and personal security has not been established. Despite this, there is growing use of social media with more than 61% using Snapchat, Instagram and Tiktok and 33% have experienced harrassment and 83.5% have been subjected to the problem of fake news (USIU Africa, 2020). Personal security aspects such as protection from physical violence, protection from cybercrime and other crimes, prevention of domestic violence, protection from exploitation e.g. child labor and job scams have not been studied in relation to various forms of social media.

Previous research has not determined relationship between forms of social media and how each form influences personal security. This relationship has not been established in literature across gender, age and socio-economic status. It has been related to cases of cyber bullying where criminals use false communication about an individual this results to cases of anxiety, depression and even suicide. Impersonation has been commonly witnessed on social media as criminals masquerade as influential leaders to dupe their victims. This research aimed to study the Social media influence on personal security among the youth in Nairobi City County as the existing gaps.

1.4 Objectives of the Study

Objectives of the current study were divided into two general and specific

1.4.1 General Objective

Social media influence on personal security among the youths in Nairobi City County

1.4.2 Specific Objectives

i. To determine forms of social media among the youth in Nairobi City County.

ii. To examine crimes that result from social media use among the youths in Nairobi City County.

iii. To analyse the influence of social media on personal security among the youth in Nairobi City County

iv. To determine challenges facing the prosecution of social media crimes among the youth in Nairobi City County.

1.5 Research Questions

i. What are the social media forms among the youth in Nairobi City County?

ii. What are the crimes that result from social media use among the youth in Nairobi City County?

iii. What is the influence of social media on personal security among the youth in Nairobi City County?

iv. What are the challenges facing prosecution of social media crimes among the youth in Nairobi City County?

1.6 Significance of the Study

This study will benefit youth, youth organizations, government and academicians. It will provide information to the youths, social media management and criminal justice practitioners. It will show how social media security can be improved and people can feel safe online without being victims of online criminal activities. The research findings will be useful to youth organizations and the national and county government in giving insights that help in prevention of social media crimes and implementation of policies to ensure online safety, further research can be conducted by academicians interested in the same field of study.

1.7 Scope of the Study

The study will be carried out among the youths in PCAK Nairobi City County being the majority in the organisation and active social media users they are also elite majority who have the knowledge of computers and smartphones. A total of 155 youths and 145 law enforcement officers in PCAK were targeted to respond to questionnaire in the current study. The study will focus on social media influence on personal security. It will leave out other aspects of social media influences not related to personal security and youth. PCAK was chosen because it is a body that registers all professional criminologists across all organizations in the security sector. Methodological scope was limited to descriptive research design with questionnaires. Inclusion criterion was membership of PCAK, both youths and law enforcement officers in Nairobi City County. Exclusion criterion was unwillingness by a member to participate based on the individual choice. Sample size of 155 youth and 145 law enforcement officers was used in the study.

1.8 Limitations and Delimitations

cation of the study was Nairobi City County among members of PCAK organisation this was chosen because it consists of several youths between the ages of 18-35 years and also has law enforcement officers who are registered criminologists. Some law enforcement respondents could not be willing to respond or be interviewed due to personal reasons. The researcher ensured that there was informed consent and confidentiality among the recipients. To mitigate these limitations, the study employed victim surveys that were meant to give assurances of confidentiality.

CHAPTER TWO

LITERATURE REVIEW AND THEORETICAL FRAMEWORK

2.1. Introduction

This chapter reviews relevant literature, empirical review, theoretical framework and conceptual framework. Empirical review presented social media and personal security. It also discussed influence of forms of social media and social media crimes on personal security. Challenges of social media as well as solutions were also reviewed. Theoretical framework was based on space transition and victim precipitation theories. The chapter also presents conceptual framework.

2.2. Empirical Review

2.2.1. Social Media and Personal Security

Various studies have addressed social media and security. A good deal of research has found that social media influences security (Gupta et al., 2018; Walsh, 2020; Walsh & O'Connor, 2019; Zhang & Gupta, 2018). According to Gupta et al. (2018), criminals use social media platforms to perpetrate crimes and violence to their target victims based on their onlione activities. Cyber criminals target social media sites by use of malware programs aimed at a computer or a network (Walsh, 2020; Zhang & Gupta, 2018). Common methods used to deliver the malicious programs are pop-up advertisements and attachments connecting to various links (Kumar & Somani, 2018). Sophos antivirus developer states that malware victims on social media are 40% of its users modern techniques target legitimate websites to spread malicious programs through holes (Kumar & Somani, 2018). Spammed emails contain malicious links that a potential victim clicks on the link which will be redirected (Soomro & Hussain, 2019)

The problem of social media security threat is compounded by computer programs that rapidly change and the increase of malicious programs making it even difficult to detect among dormant computers (Radunović & Veinović, 2020). Cyberbullying perpetrators may enjoy anonymity due to the fact that they can change user profiles and personal information of different individuals (Nilan et al., 2015). According to Nilan et al. (2015), the victim maybe aware of the offender but challenge is posed when proof is required to show indeed the offender is someone well known to the victims. Online romance scams occurs when a user sends friend request to someone pretending to show interest, they end up exchanging personal information that is used to manipulate their victims for monetary gains (Whitty & Buchanan, 2016). Studies carried out show that social media users or someone they know has experienced online romance scams with the users forging new relationships online(De Jong, 2019). Loneliness has been attributed to victims who get involved in online romance scams a study carried out shows that most victims are females (Shaari et al., 2019).

All these studies focus on various social media crimes and threats to security. The problem is that the reviewed studies do not clearly address relationship between different forms of social media and personal security. There is therefore need to establish how different aspects of personal security are influenced by various forms of social media.

2.2.2. Social Media Forms and Personal Security

Previous literature has addressed different forms of social media (Elsaesser et al., 2021; Manyerere, 2021; Pawelz & Elvers, 2018; Tanvir et al., 2021) . According to Arigo et al. (2018), each form of social media has specific privacy and account settings to suit the target market WhatsApp contains end to end encryption that prevents information access to third parties (Tamori et al., 2018). Facebook security concerns include hacking of user accounts, impersonation, cyber bullying and cyber stalking. Several years after Facebook inception user

name and passwords were sent with encryption making it available for third parties hence a security risk (Calbalhin, 2018). According to Dhami, et al. (2013), in their study of Orkut, Facebook, Google+, Twitter, there are significant privacy concerns relating to Facebook such as security risks and trust. The study relied on data and information from 250 accounts of people of varying ages in India, therefore, did not solely focus on youth (Dhami et al., 2013). Whereas privacy is an aspect of personal security, the research left out other aspects of personal security and did not substantively address it.

Security concerns on WhatsApp include sharing links to different users that are malware attacks and when followed could lead to the users details leaked, also most computers, tablets and smart phones do not encrypt data such as iPhones hence posing a security risk (Arigo et al., 2018). Identity theft occurs when a person for example stealing someone's phone and sending messages to the contacts to obtain money (Irshad & Soomro, 2018). Research on use of social media suggests that social uses top the list such as exchanging of emails and chatting, the highest percentage of people have email accounts (Nishad, 2018). Cyber criminals send emails with the motive of defrauding their victims or invite them for a false interview that the mainstream organisation knows nothing about. Some go as far as collecting application fee from unsuspecting job seekers in order to be recruited (Hufnagel et al., 2019).

Though the reviewed literature link social media use to security, it fails to focus on the youth and also fails to address personal security. The review literature does not address the influence of social media on protection from physical violence, domestic violence, exploitation and scams that are aspects of personal security. Studies that address these aspects do not give clear relationship between them and social media and are not substantive (Cross et al., 2018; Makinde et al., 2021; Paat & Markham, 2021).

The studies reviewed do not address the influence of various forms of social media on personal security. The studies also fail to disaggregate the security threats of social media platforms by

offender and victim gender and ages. There is need to have such insight in order to understand the influence and relationships.

2.2.3. Social Media Crimes and Personal Security

Social media crimes have been on the rise, this is due to the increase of cyber criminals who take advantage of anonymity(Dubord, 2008). Lack of deterrence factor and identity flexibility, in America bad behaviour promoted on Facebook has led to more serious crimes such as rape and assault several users have lamented on no efforts from Facebook teams to end the violence pages by closing them down (Brainard, 2018). Compromising photographs of individuals have been posted on Facebook and before they are removed the damage will have already been done as they will be downloaded and saved in individual devices (Wang & Mark, 2018).

NW3C outlines six types of crimes in the cyber space these are social media burglary, social engineering, computer fraud, identity theft, cyber-casing and cyber-stalking (Soomro & Hussain, 2019). Cybercriminals look for information from social media users before conducting burglary especially when the victims post that they are in a different location. Phishing emails are sent to victims with the aim of getting useful information such credit numbers and passwords, criminals use social networking sites to ask for urgent financial assistance (Soomro & Hussain, 2019)

The youth are at risk of social media crimes that include cyber bullying, study carried out showed that Facebook had the highest percentage of cyber bullying followed by twitter most of the cases happen to females (Abaido, 2020). The cases often go unreported due to fear and social stigma this results to depression, anger, anxiety, psychological and emotional issues and suicidal thoughts (Abaido, 2020). Study carried out on university students in Malaysia cyber bullying caused them emotional and psychological stress then led to drop in academic performance, most of the victims were females more than males (Ruangnapakul et al., 2019).

Most of the victims choose not to reveal the experience to anyone for lack of assistance or when the damage has already been done, cyber bullying also decreased with an increase in age (Ruangnapakul et al., 2019).

Social media crimes are becoming increasingly more common with issues such as data breaches more prominent. Researchers have found fundamental flaws in security protocols like the OpenSSL Heartbleed Bug and the successful site attacks by hacker groups. New threats and challenges are also emerging continually with emerging technologies like IoT, Big Data etc. The cyber crime incidences of spear phishing are also on the increase and involve the installation of harmful malware on the computer or device and stealing valuable and sensitive information.

Social media criminals target individuals through phishing emails. The phishing emails are used to install ransomware that spread via hacked or compromised sites. Ransomware encrypts files of the victims, and cause damage. The rate of ransoms also depends on the type of social media, organizations or persons, and the security experts are finding it difficult to protect the platforms and sites.

2.2.4 Social Media and Personal Security

Social media affects personal security either positively by providing information to law enforcers and the general public by profiling criminals (Walsh & O'Connor, 2019). Negative effects which are majority are guided by the threats to personal security which can be witnessed on social media, armed conflict threat is experienced on social media whereby terrorist groups use social media to communicate to their sympathizers while creating fear to the general public by taking responsibility to attack (Muindi, 2020). Crime as a second threat to personal security is widely experienced on social media ranging from cyber bullying, identity theft, phishing and cyber stalking (Soomro & Hussain, 2019) The third and final threat is drugs, substance abuse

and suicide social media has provided an opportunity for drug users to post alcohol and drugs hence portraying a negative image to others who will feel (Wakoli, 2018).

Victims are exposed to online crimes by the fact that they belong to the networks, the cyber criminals will target an individual and expose their personal photos online for everybody to see (Henson et al., 2016). The situation may worsen as other members may join the criminal by condemning the victim and judging them others go as far as tagging close family members and friends (Olivas, 2019). The victims rarely share with adults for the fear of being judged this may later lead to repeat victimisation (Aizenkot, 2018). The effects of cyber bullying include dropping out of school, drugs and substance abuse, depression and suicide (Nikolaou, 2017).

Gender differences in terms of bullying shows that males are actively involved in the bully group compared to females who are majority in the victim group this is attributed to male aggressive behaviour which is socially acceptable (M. Jaradat, 2017). Feminist scholars argue that the internet perpetrates crimes against females and therefore they are likely to be victims (Ramirez & Denault, 2019).

2.2.5 Challenges of Social Media Security and Solutions

Criminals and various terrorist organisations use social media to propagate and recruit new members into their groups (Darden, 2019) .Structural and leadership challenges among Indian law enforcement officers have been reported. Most of the police forces are colonial and therefore resistant to making necessary changes that come with technology, lack of trained personnel and equipment to facilitate in investigation is equally a challenge (Hu & Lovrich, 2019). Nigerian law enforcement officers face public interference during investigation on social media through circulation of false information, few or lack of training among law enforcers has posed a great challenge in social media investigation and prosecution (Peters & Ojedokun, 2019)

Different social media forms have specific privacy settings that the users put in place to minimize cases of victimization. Personal information can be restricted to an individual or few trusted friends(van Schaik et al., 2018), however cases have been reported where an account has been hacked even with the existing privacy mechanisms and password changed so it may not be safe as perceived. A framework has been developed to handle privacy concerns called reputation mechanism which interprets the semantics then provides positive and negative results which can be recommended to a new user (Almarabeh, 2019).

Users should install up to date antivirus software to prevent malicious programs, email address used in social media site should be different from workplace emails(Soomro & Hussain, 2019) To prevent cyber stalking also utilise the available security settings on social media sites to reduce the chances of being targeted. When using a smart phone ensure that the GPS is switched off that may show the offender your exact location (Almarabeh, 2019). Cyber criminals are more intelligent than the physical criminals before committing a crime they take time to study their targets including their interests, work places and homes. Innocent victims post on social media that they have travelled to the village so the offender will be aware of the absentee guardian taking advantage of the situation to commit crimes like burglary (Soomro & Hussain, 2019).

Social media laws should be made to cater for individuals who have lost their lives so that they families can be allowed to access their accounts then log out or deactivate instead of the accounts remaining active in the case where the individual did not share the password details (Kalule, 2018).

Despite the attempts to address challenges, the threats of social media to personal security remains a problem. The reviewed literature provides appropriate measures but do not address the challenges with respect to all dimensions of personal security. The previous research also fail to address peculiarities of the problem with regard to youth, gender and local perspectives.

2.3 Theoretical Framework

This section presents a review of the framework of theories upon which the research was grounded. The research was grounded on Space Transition and Victim Precipitation theories. Each of these theories together address the concept of social media use and personal security and are therefore justified to be used in the current study.

2.3.1 Space Transition Theory

Jaishankar proposed a new theory of cybercrime in 2008. Space transition theory explains criminal behaviour both in actual space and cyber space (Jaihankar, 2008).

Criminals are likely to commit crime in virtual space due to flexible identity, impersonation and lack of deterrence factor. Criminal behaviour in digital space may likely to be transferred to actual space. This theory states that criminals are likely to meet in the virtual space due to their similarities in goals then agree to participate in crimes as a group, the platform provides an easy way for escape due to the temporal nature of cyber space. Cybercrimes may result from the conflict of norms from physical space and cyberspace .This theory gives and explanation to what leads to cybercrime and the nature of behaviour of offenders in the cyber space.

In this study, social media sites provide avenues for criminals to commit crimes identity is flexible due to the fact that they can create profiles using fake name and even put fake photographs which can be easily accessed online. When a crime is committed the victim may not have the details of the offender. Cybercrimes laws in Kenya have not been fully implemented and this poses a challenge to the victims who have to endure the wrath of the perpetrators for fear of being exposed to the whole world. Black mail is a common characteristic of online criminals they demand monetary gains or damage the victim’s reputation

2.3.2 Victim Precipitation Theory

The theory was first introduced in twentieth century by Marvin Wolfgang and perfected thereafter, Siegel (2006) attributes to individual interests and behaviour that likely subject them to be suitable targets. The theory states that victims through their actions predispose themselves to be suitable targets to perpetrators.

The theory relates to this study for instance on social media, posting of personal information provides crucial information to the perpetrators. Posting photographs and status updates suggesting the location will also give a clue to the cyber criminals. Posting online travel information may give a clue to the attackers who will be aware that the home is left without a guardian and there will be easy access (Petherick, 2017).

Offenders form false accounts to frustrate their victims without being recognised. Active precipitation attributes to the fact that the victim is aware of the offender women who send half naked photographs to the social media sites may have contributed to any criminal activity directed towards them, the cyber bullies will end up branding them as prostitutes. Passive precipitation occurs when the victim is not attacked directly for example a group directed to ruin the reputation of an opponent so that they lose in elections.(Petherick, 2017)

2.4 Conceptual Framework

It is a model that deals with variables and their relationships, the dependent, independent and intervening variables. Forms of social media being the independent variables measured in in terms of network types. The intervening variables include victim predisposition, presence of vulnerabilities, lack of specific legal framework and inadequate capacity of law enforcement. Enabling resources are the electronic gadgets and internet connection, the dependent variables of personal security which would be measured in terms of personal security influences. These influences on protection from physical violence, protection from cybercrime and other crimes,

prevention of domestic violence, protection from child labor and scams as well as password security.

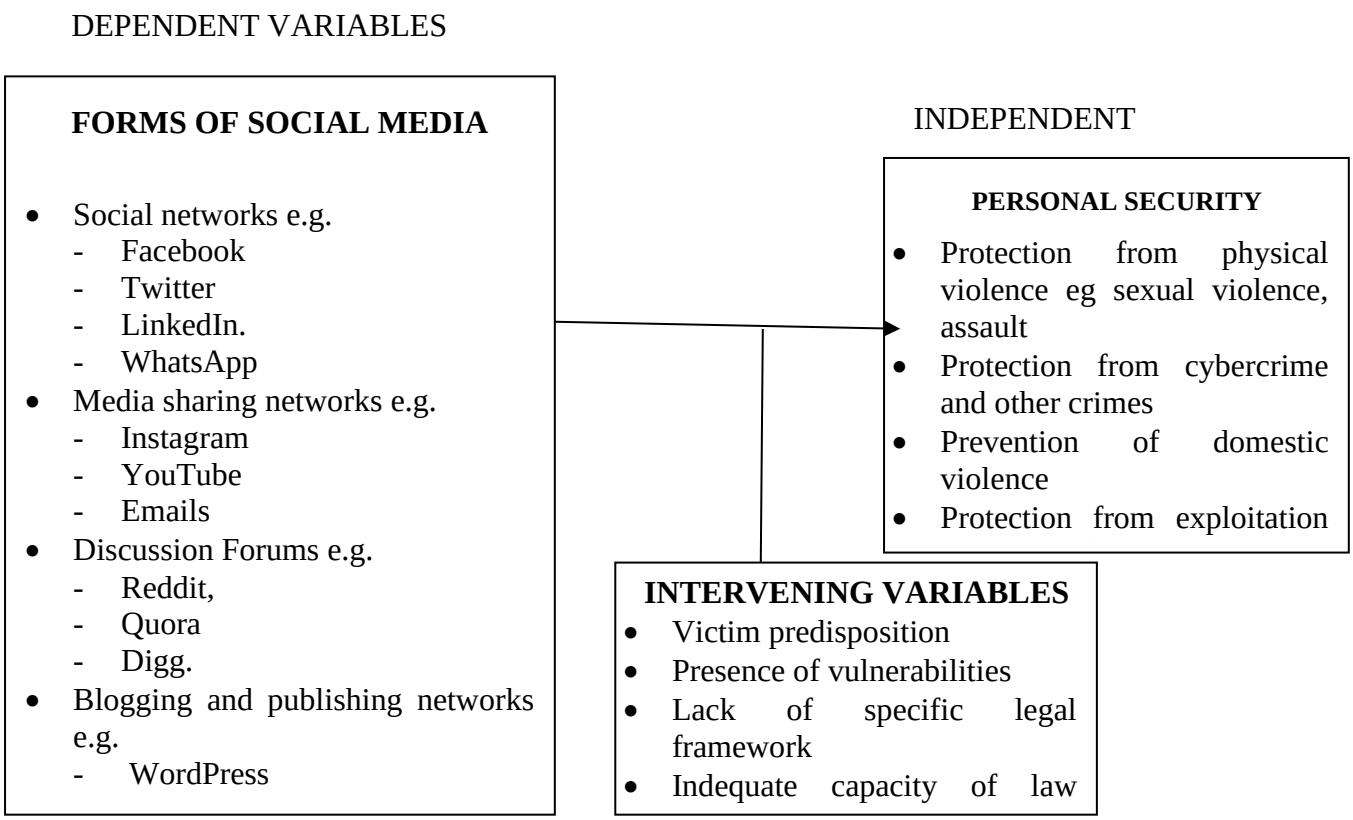


Figure 2.1: Conceptual framework

(*Source:* Researcher)

CHAPTER THREE

RESEARCH METHODOLOGY

3.1. Introduction

This chapter covers the following: research design, study site, target population, sampling procedure, sample size, data collection instruments and ethical considerations.

3.2 Research Design

This study employed a descriptive survey research. The design was chosen as the population was to be described with respect to study variables. Kerlinger and Lee (2000) assert that descriptive design is appropriate to comprehensively gather information of a specific group at an appropriate time and location. It also adopted a mixed-method approach, which aims to obtain quantitative and qualitative data required in the study according to the objectives (Silva, 2017). Both quantitative and qualitative data was collected using survey questionnaires distributed among the respondents then later on analysed.

3.3 Study Site

The study was geographically located in Nairobi City County, Kenya. The site was selected as it is a cosmopolitan area with majority of the population from diverse backgrounds. The city is also preferred due to its connectivity and large use of social media as well as due to issues of security. The Professional Criminologists Association of Kenya was selected as an organization with members whose practice address crime in Nairobi City County. The members who participated in filling questionnaires were between ages 18-35 years.

3.4. Target Population

Target population is a group of people with common characteristics that meet the criteria for a specific research topic (Mohsin Alvi, 2016). Target population for this study was all youth and

law enforcement officers in Nairobi County and who were members of PCAK. Target population was 17,000 persons including 15,000 youths in the age bracket of 18-35 years and 2,000 law enforcement officers in PCAK in Nairobi. Tables 3.1 and 3.2 illustrate the respective target population.

Table 3.1 : Target population of youth members of PCAK

Youth Respondents by Age	Target Population		
	Female	Male	Total
19-25	2,710	8,032	10,742
26-30	677	2,226	2,903
31-35	387	968	1,355
Total	3,774	11,226	15,000

(*Source:* PCAK, 2021)

Table 3.2: Target population of law enforcement members of PCAK

Law enforcement Department	Target Population		
	Female	Male	Total
Administration Police Service	273	230	503
Kenya Police Service	480	343	823
Directorate of Criminal Investigations	178	233	411
Private Security Services	94	80	174
Others	42	57	99
Total	1,067	933	2000

(*Source:* PCAK, 2021)

3.4.1 Inclusion Criteria

The study involved members of PCAK, both youths and law enforcement officers in Nairobi City County.

3.4.2 Exclusion criteria

The members who were not willing to be interviewed or to respond to questionnaires did not take part in the study as it is based on the individual choice.

3.5 Sample Size

Sample size calculation was based on the following formula (Nassiuma, 2000) where N represents the population, n=sample size, C= coefficient of variance, e= standard error.

$$n= \frac{NC^2}{C^2+(N-1)e^2}$$

Sample size for youth respondents was calculated as shown below.

C=25% acceptable, e=0.02 and N = 15000

$$n= \frac{15000*0.25^2}{0.25^2+(15{,}000-1)0.02^2}$$

$$n= \frac{937.5}{6.0621}$$

$$n=154.65$$

n=155 youth respondents

Sample size for youth respondents was calculated as shown below.

C=25% acceptable, e=0.02 and N = 2000

$$n= \frac{2{,}000*0.25^2}{0.25^2+(2{,}000-1)0.02^2}$$

$$n= \frac{125}{0.8621}$$

$$n=144.99$$

n=145 law enforcement informants

Sample size for youth and law enforcement informants were found as illustrated in Tables 3.3 and 3.4.

Table 3.3: Sample size for youth respondents

Youth Respondents by Age	Sample Size		
	Female	**Male**	**Total**
19-25	28	83	111
26-30	7	23	30
31-35	4	10	14
Total	39	116	155

(*Source:* PCAK, 2021)

Table 3.4: Sample size for law enforcement informants

Law enforcement Department	Sample Size		
	Female	**Male**	**Total**
Administration Police Service	19	16	35
Kenya Police Service	35	25	60
Directorate of Criminal Investigations	13	17	30
Private Security Services	7	6	13
Others	3	4	7
Total	77	68	145

3.6 Sampling Technique

Sampling involves extracting a smaller number also referred to as a sample from a population (Mohsin Alvi, 2016).The selected sample provided representation of the whole population and should have similar characteristics. Stratified random sampling technique was used to select 155 youths and from a sample size drawn from the population of 15,000 PCAK youths and 145 respondents from population of 2,000 PCAK law enforcement officers. Stratified random sampling technique was selected because of its ability to capture key population characteristics in the sample using a weighted average for each stratum to be proportional to the overall

population. The strata for law enforcement were their organizations and gender while that of youth was age and gender.

3.7 Data Collection Instrument

Primary data were collected using questionnaire administered by the researcher and a research assistant. Both quantitative and qualitative data were collected. A sample of the questionnaire is attached as appendix II. The questionnaire was administered to the members of PCAK to get answers on the social media influence on personal security among the youths in Nairobi County. Law enforcement officers provided information related to the challenges involving prosecution of social media crimes and sample questions were attached as shown in Appendix III.

3.8 Validity and Reliability

3.8.1 Validity

This the extent to which a concept can be accurately measured (Heale & Twycross, 2015). The researcher determined content validity by ensuring the instrument in the study covers all the content variables verified along research objectives. The supervisor compared the research instruments in relation to appropriateness, ethical considerations and suitability to research objectives then recommend changes.

3.8.2 Reliability

Reliability is the consistency of measures while undertaking a study. (Heale & Twycross, 2015). A pilot study was carried out with 10% of sample size (30 respondents) to test the reliability of research instruments. The respondents were given questionnaires twice and responses were analyzed. The researcher sampled feedback from questionnaires issued to different groups and analysed the correlation based on responses given. The researcher assessed internal consistency using Cronbach alpha score. Results of computation of Cronbach alpha score of the pilot study

showed that the reliability was above 0.7 meaning that the data collection instruments were highly reliable.

3.9 Data Collection Procedure

An introductory letter from the graduate school with a research permit was presented to the offices of PCAK located in Nairobi City County to inform them about the study and the intention to collect data. The researcher worked with the management of PCAK to provide directions on how to get the members to receive questionnaires and to be interviewed. The Questionnaires were administered with the help of a research assistant and respondents were given time to fill.

3.10 Data Analysis and Management

The questionnaire was cross-checked for completeness and data cleaning. Respondents were requested to fill gaps if identified during data collection to improve the quality of the responses. The responses were summarized and coded using Statistical Package for Social Sciences (SPSS).

Data analysis was done using quantitative and qualitative methods. Qualitative data analysis was carried out by summarizing, interpreting data in correct way through text nferencing using methods of nferential statistics, reviewing and generalizing (Harding, 2018; Kuckartz, 2019). SPSS was used in descriptive statistics such as frequencies of responses. Qualitative data collected from secondary sources and from primary sources in open ended questions in questionnaire were analyzed using qualitative means as indicated by which include close reading, sequential text interpretation, coding, organizing and sorting data and quering data using Boolean, semantic and proximity operators (Friese, 2019). Graphs, charts and tables were used to represent data.

3.11 Ethical Considerations

These are set guidelines admissible when conducting a study, before conducting the study the researcher followed the university requirements and applied for research permit from NACOSTI. The researcher sought permissions from the University and license from NACOSTI in order to start data collection. The target respondents were asked for permission to conduct research.

As part of informed consent process, the researcher described the study purpose and objectives and explained why the contribution of respondent was important. The respondents were sent the introductory emails and informed that the research was on voluntary basis with the information being used solely for academic purposes. The respondents were assured that the information they were to provide would not be released to any third party. They were not required to disclose their identities if they did not wish to do so to ensure privacy and confidentiality of the information shared. The researcher ensured that the methodology used to carry out research led to unbiased conclusions by gathering information with integrity. The researcher did not lead the respondents to a desired outcome of the study objectives. The data collected were kept discreet only to be accesed by the researcher and supervisor for research purpose only.

There was no compensation to participants. Participants were encouraged to be very truthful in their responses to avoid misleading the researcher. They were required to disclose any information relevant to study and to only give information that was allowed to be given. Confidentiality was guaranteed to the respondents in case of any disclosure that required that measure.

The researcher ensured administrative safeguards to protect the privacy of participants' information by clearly delineating who did and who did not have access to participants'

information. The number of individuals that had access to private and confidential information was very limited to ensure privacy and confidentiality of participants' information. Technical safeguards were also implemented to protect the privacy of participants. The measures included the use of computer passwords, firewalls, anti-virus software, encryption and other measures that protected data from unauthorized individuals, loss, theft or modification. The researcher ensured that research design had safeguards to protect the privacy of research participants. The researcher anonymized information, transcribed raw data as required, stored de-identified data separately from coding lists, any hard copy with sensitive information was shredded as soon as feasible, and so on.

There are three circumstances where the duty to protect the privacy and confidentiality of participants' information may be limited as a result of other competing factors. In cases where measures adopted to protect the privacy of participants was inimical to the integrity of the research design, where the researcher was under a legal responsibility or a duty to report participants' information to the authorities; and where respecting the confidentiality of participants' information undermines the autonomy of research participants. In the current research, the researcher disclosed the privacy and confidentiality risks to potential participants inherent in their participation in the consent form and also in email correspondence. This was in situation where adoption of measures to protect the privacy was found inimical to the integrity of the research design. Information such as email addresses and phone numbers could be disclosed to supervisors if allowed by the University and the respondents.

CHAPTER FOUR

DATA, ANALYSIS, PRESENTATION AND DISCUSSION OF FINDINGS

4.1. Introduction

The chapter deals with presentation, analysis, interpretation and discussions of findings. Results of this research were presented in form of frequency tables, graphs and pie charts. The results were discussed to generate logical conclusions in relation to objectives of the study.

4.2. Response Rate

The general response rate for all the participants in the current study was 43.00% where 129 out of 300 targeted respondents participated as shown in Table 4.1. Response rate for youth respondents drawn from PCAK was at 43.23% with 67 out of 155 target respondents participating. The response rate of the law enforcement informants drawn from PCAK was 42.76% with 62 out of 145 targeted respondents participating.

The response rate found in the current research was well above the average response rate for surveys that was found as 33% as shown in Lindemann (2021). The response rate in the current was also above the acceptable limit for online surveys that was found as 29% (Lindemann, 2021). It was found out that the response rate for youth participants was slightly higher than that for law enforcement informants possibly due to previous finding that young people are frequently use internet than older people (Kelfve, Kivi, Johansson, & Lindwall, 2020). The finding confirms findings in previous research that youth more efficiently use online questionnaire than older people who often find being online challenging (Dillman & Smyth, 2007; Kaplowitz, Hadlock, & Levine, 2004).

Table 4.1: Response rate

PCKA Members	Sample			Participants			Rate (%)
	Male	Female	Total	Male	Female	Total	
Youth	116	39	155	50	17	67	43.23%
Law enforcement	77	68	145	51	11	62	42.76%
Total	193	107	300	101	28	129	43.00%

(*Source:* Researcher)

4.3. Respondents' Demographic Characteristics

4.3.1. Gender

Table 4.2 illustrates that male youth respondents were 74.63% of the total number of participants. Out of 67 youth respondents, only 17 (25.37%) were female and out of 62 law enforcement informants, only 11 (17.74%) were female. This shows that larger percentage of female youth respondents participated in this research than that of female law enforcement informants. The converse was true for the male youth and law enforcement informants. In the current research, number of male youth was greater than that of male law enforcement officers in the sample yet less number of male youth participated.

The reason for low percentage of female respondents was thought to be as a result of gender inequity in PCAK. This view relates to finding by Smith (2008) that gender differences in the way females and males respond in online surveys reflect the way females and males values operate in social exchange resulting into disproportionate number of female respondents in the surveys. The results of this research also corroborate findings of Wambua (2020) who carried out study of social media impact on security in Kenya and found that male respondents were more than female respondents and it reflected the population studied.

Finding in the current research that a greater percentage of male in law enforcement responded to the online questionnaire compared to that of male youth suggests similar finding in literature that male law enforcement officers were more involved online than their youth counterparts possibly due to their active duty in crime prevention in this age of increased cybercrime as a basis for engagement with the public (Crump, 2011; Lieberman, Koetzle, & Sakiyama, 2013).

Table 4.2: Respondents by gender

Gender	Youth Respondents		Law enforcement informants		Total	
	Frequency	Percent	Frequency	Percent	Frequency	Percent
Female	17	25.37	11	17.74	28	21.71
Male	50	74.63	51	82.26	101	78.29
Total	67	100.00	62	100.00	129	100.00

(*Source:* Researcher)

4.3.2. Education

Figure 4.1 illustrates highest level of education of youth respondents. About 96% of the respondents had university education while the rest had college and tertiary education or were students of relevant criminology courses. This high percentage of youth respondents with university education was due to registration requirements of PCAK which makes it mandatory for all members to have studied course related to criminology and/or have passed vetting and approval process (PCAK, 2021).

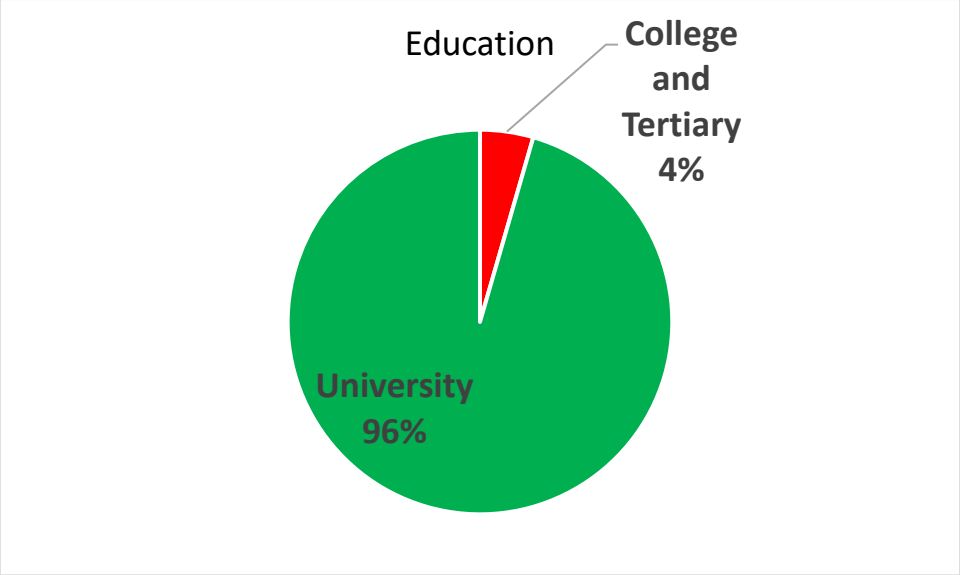


Figure 4.1: Education of youth respondents

(*Source:* Researcher)

4.3.3 Age

Figure 4.2 illustrates age distribution of the youth respondents. About 72% were in the age bracket of 18-25 years, 19% were in the age bracket of 26-30 years and the rest were in the age group of 31-35 years. Figure 4.2 also shows that those aged between 18-30 years were 91% while those aged above 30 years were only about 9%. The percentages of youth respondents reduce with increase in age. This distribution mirrors the population and the sample of youth in the current study.

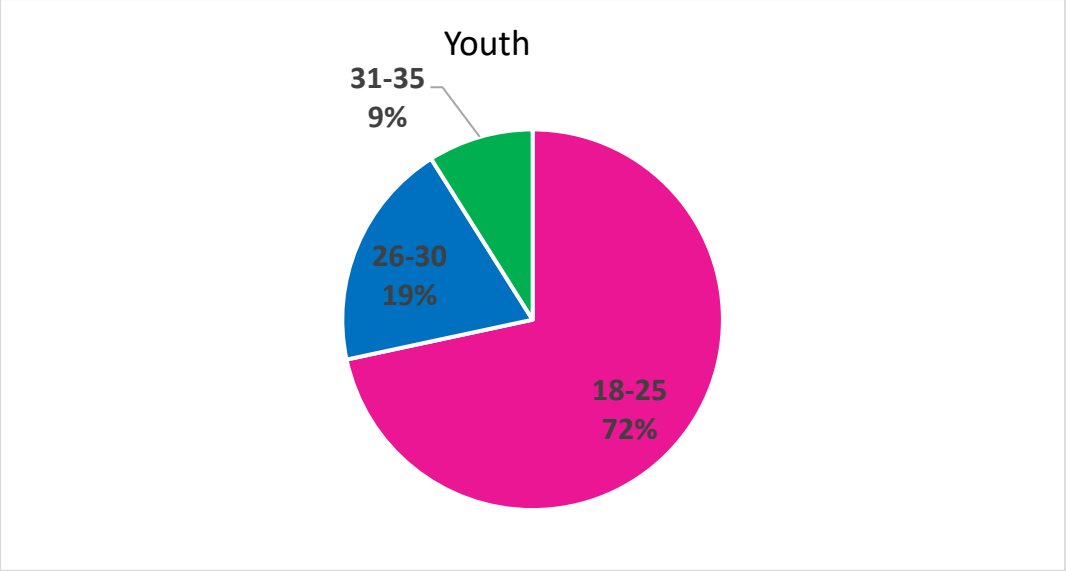


Figure 4.2: Age distribution of youth respondents

(*Source:* Researcher)

Figure 4.3 illustrates age distribution of the law enforcement informants. About 58% were in the age bracket of 31-40 years, 18% were in the age bracket of 41-50 years, 18% were in the age bracket of 21-30 years and the rest were above 50 years. Figure 4.3 also shows that those aged between 21-50 years were 94% while those aged above 50 years were only about 6%.

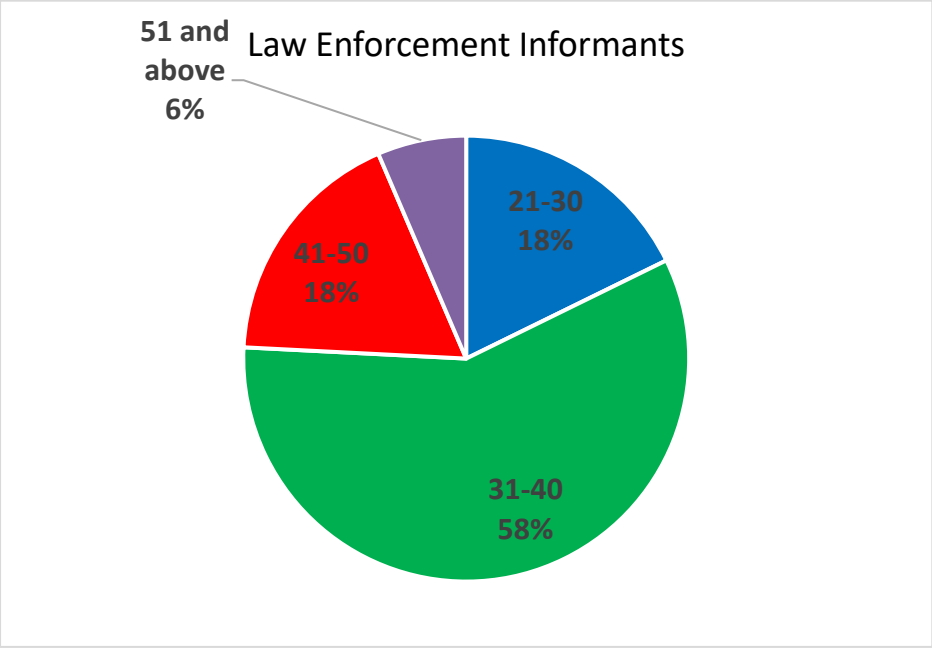


Figure 4.3: Age distribution of law enforcement informants

(*Source:* Researcher)

The findings generally show that youth of 30 years and below formed a larger percentage of respondents (91%) compared to their older counterparts. A similar result (94%) was found for law enforcement officers who were 50 years and below. This was a reflection of the population and the sample of the current research.

4.3.3. Occupation of Youth Respondents

Results presented in Figure 4.4 illustrate that about 36% of the youth respondents were job seekers while 37% were students. About 27% of the youth respondents were employed. It means that about 73% were unemployed, either still studying or seeking employment. The findings are contrary to those by Wambua (2020) whose results were that about 17% of the youth respondents were unemployed. However, the nature of sampling carried out by Wambua (2020) was not clear in her report, but must have impacted on the sample percentages. The percentage of unemployed job seekers in the current research (36%) was found to be close to national percentage of unemployed youth that was rated at 39% in the 2019 Census (KNBS, 2019).

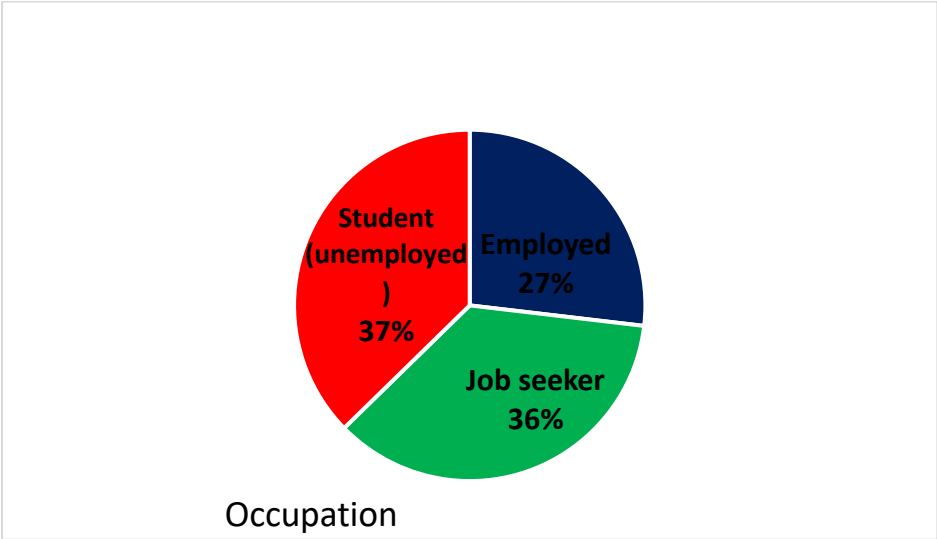


Figure 4.4: Occupation status of youth respondents

(*Source:* Researcher)

4.4. Descriptive Findings

4.4.1. Forms of Social Media Among the Youth in Nairobi City County

Pie chart in Figure 4.5 illustrates that 84% of the youth respondents indicated that they mostly used WhatsApp, about 6% of them commonly used Twitter, 4% used Instagram, 3% used Facebook and the rest mainly used emails. From these results, about 97% of the youth respondents used WhatsApp, Twitter, Instagram and Facebook and only 3% commonly used other social media platforms such as emails and LinkedIn.

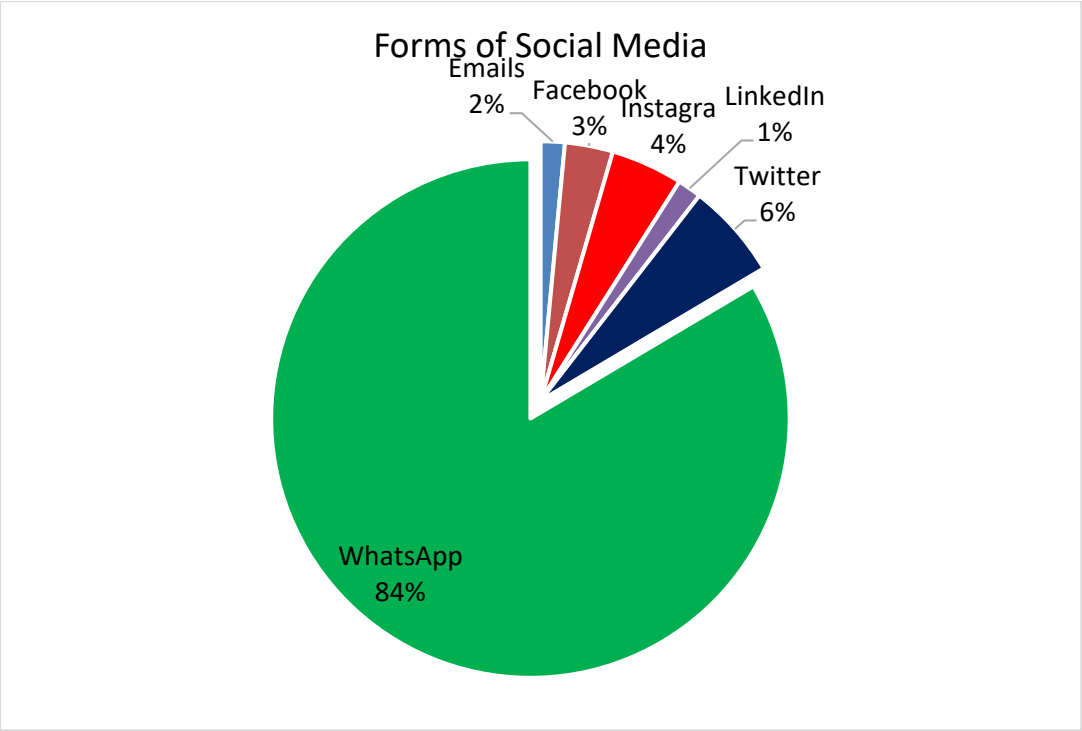


Figure 4.5: Most commonly used forms of social media among youth

(*Source:* Researcher)

The results that the youth prefer WhatsApp over other social media platforms corroborate findings in previous research that it provides simple, personal and real time messaging without any cost other than their internet data already in their smart phones (Jisha & Jebakumar, 2014; Udenze, 2017). Percentage usage of WhatsApp was closer to that found in a study in Kenya that found its use at 89% compared to 84% found in the current research. (SIMElab Africa,

2019) Instagram, Facebook and WhatsApp are all owned by Facebook Inc and were most commonly used by 91% of the youth respondents. The largest preference of WhatsApp by the youth in the current research was also most likely due to its privacy features enabled by end-to-end encryption confirmed by Endeley (2018) as a means of preventing privacy infringements and reducing security threats due to hacking and other cybercrimes.

Further analysis of forms of social media used with respect to gender is shown in Figures 4.6 and 4.7. About 86% of male and 76% of female youth respondents were found to mostly use WhatsApp. About 4% of male and 12% of female youth respondents were found to mostly use Twitter. Similar results were found with regard to Instagram where more female youth respondents (12%) used Instagram compared to male who were only 2%.

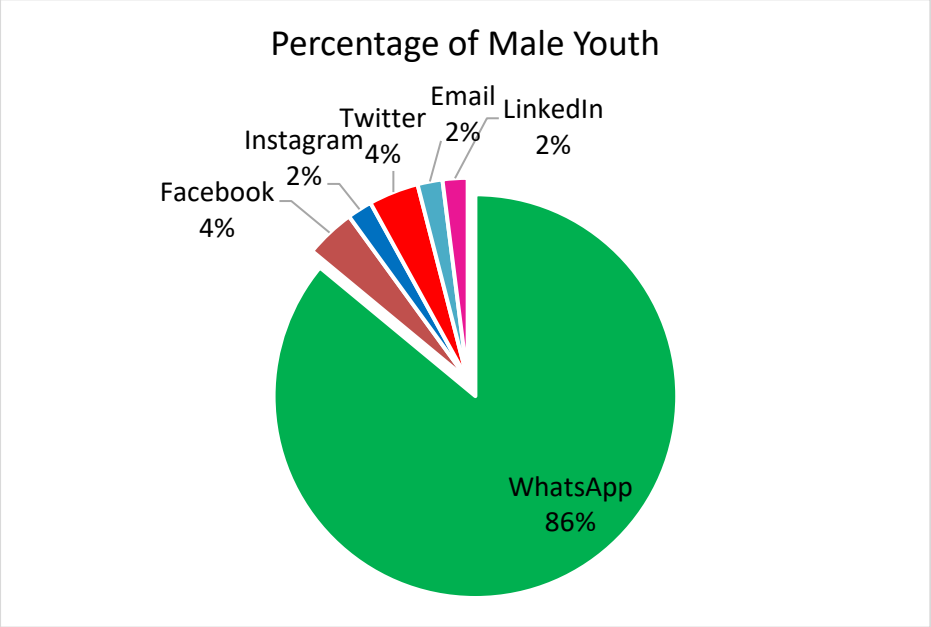


Figure 4.6: Forms of social media mostly used by male youth respondents

(*Source:* Researcher)

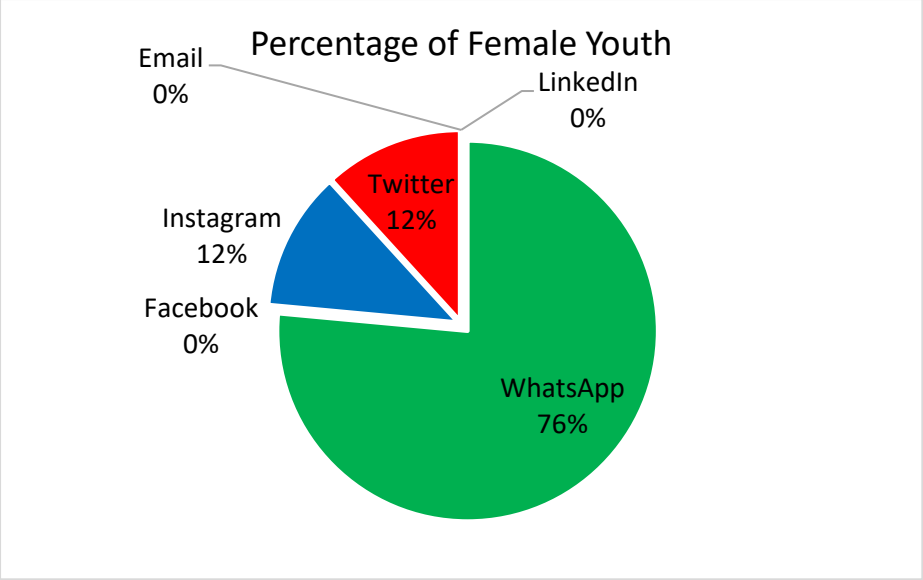


Figure 4.7: Forms of social media mostly used by female youth respondents

(*Source:* Researcher)

From the results it was clear generally that the most preferred social media platforms by both gender was WhatsApp and Twitter. This finding on youth preference of WhatsApp and Twitter corroborate findings in previous research (Aissani & Dheyab Abdullah, 2018; George, Sabu, & Jamir, 2020). Additionally, male youth respondents mostly preferred Facebook while female youth respondents mostly preferred to use Instagram. This finding confirm previous findings of Waechter (2021) in his study of social media individuality and collectivity that female youth prefer Instagram more than their male counterparts . The results that female youth mostly preferred Instagram to Facebook compared to the male also confirm findings by Herrero-Diz and Ramos-Serrano (2018).

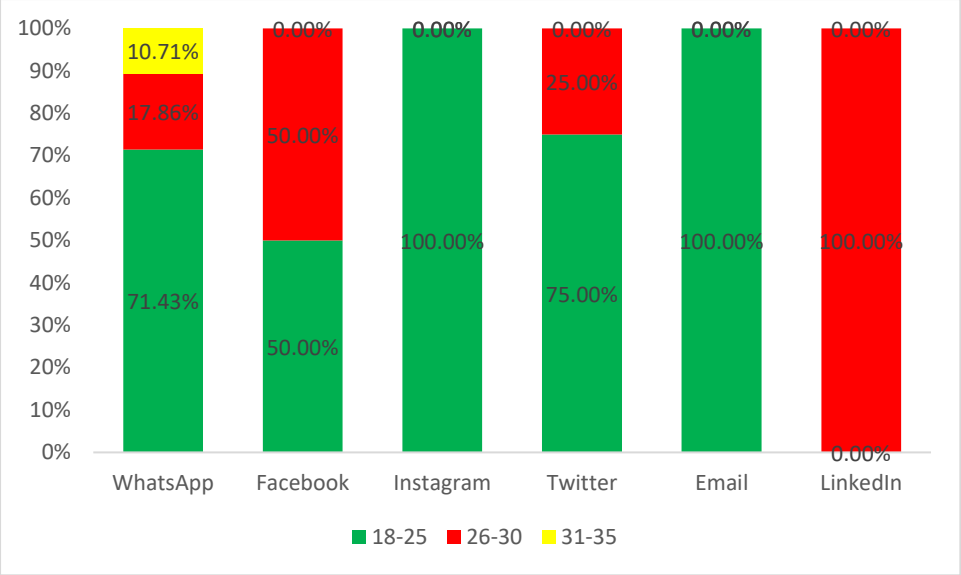


Figure 4.8: Youth preference of forms of social media by age

(*Source:* Researcher)

Analysis of social media preference across age groups of the youth respondents presented in Figure 4.8 illustrated that Instagram and Email were preferred by youth in the age bracket of 18-25 years while LinkedIn was most preferred by youth in the age bracket of 26-30 years. From the results, about 75% of youth that preferred Twitter were in the age group of 18-25 years while the rest who preferred the platform were 26-30 years old. Facebook was preferred in equal measure by youth respondents aged 18-25 and 26-30 years. About 71.48% of youth who preferred WhatsApp were in the age bracket of 18-25 years, 17.86% were in the bracket of 26-30 years and the rest were in the bracket of 31-35 years.

The findings show that older youth in the age group of 31-35 years did not prefer Facebook, Instagram, Twitter, Email and LinkedIn but preferred WhatsApp. This could possibly be due to privacy of WhatsApp and its convenience in communicating with friends and group members as indicated by Udenze (2017). WhatsApp, Facebook, Twitter, Instagram and Emails were most preferred by younger youth in the age bracket of 18-25 years possibly corroborate findings of Uls, Ellison and Sunrahmanyam (2017) in their study of benefits and costs of social media in adolescence. They indicated that youth needed the platforms for frequent

communication, relationships, job-search, sharing study materials for those who are students and for sending of important documents (Uhls, Ellison, & Subrahmanyam, 2017).

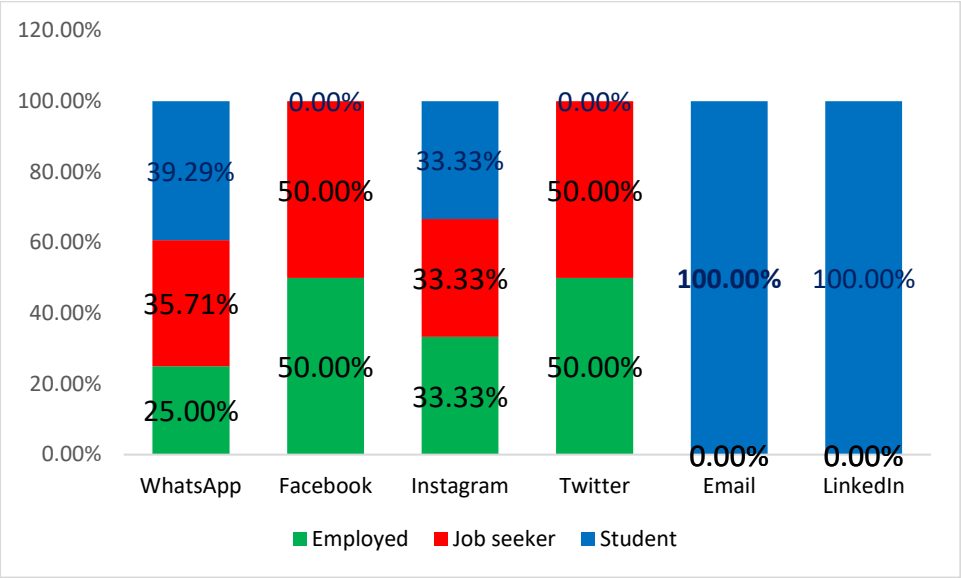


Figure 4.9: Youth preference of forms of social media by occupation

(*Source:* Researcher)

Analysis of social media preference across occupation status of the youth respondents presented in Figure 4.9 illustrated that all the youth across occupations preferred WhatsApp and Instagram. In addition to the two platforms, employed youth respondents preferred Facebook and Twitter while job seekers preferred Facebook and Twitter and students mostly preferred Email and LinkedIn.

Focusing on each platform, Email and LinkedIn were preferred by students. Facebook and Twitter were preferred equally among job seekers and employed youth respondents. Instagram was also mostly used in equal measure of 33.33% among each of the groups. About 39.29% of youth who mostly used WhatsApp were students, 35.71% were job seekers while 25% were employed.

The findings that job seekers WhatsApp, Facebook, Instagram and Twitter to Emails and LinkedIn show that they possibly used these social media to cultivate their social support

networks as suggested by literature (Feuls, Fieseler, & Suphan, 2014). However, the finding that LinkedIn and Emails were not preferred among job seekers but are entirely preferred to other platforms by students was surprising, and suggests that job seekers are mainly focused on maintaining support networks and not in active formal pursuit of jobs by use of emails and LinkedIn which, according to Chytiri (2015) and Bichir (2011), are preferred by employers.

4.4.2. Crimes that Result from Social Media use among the Youths in Nairobi City County

Results in Figure 4.10 show percentage distribution of respondents based on their opinion on most insecure social media platform. About 84% of youth respondents had opinion that Facebook was most insecure, 6% had similar opinion on Instagram, 4% on WhatsApp, 3% on emails and the rest on YouTube. In total, only 16% of respondents believed that other platforms, apart from Facebook, were most insecure. The finding that Facebook was the least secure corroborates findings in literature by Donoghue (2017) in his doctoral dissertation that studied youth students.

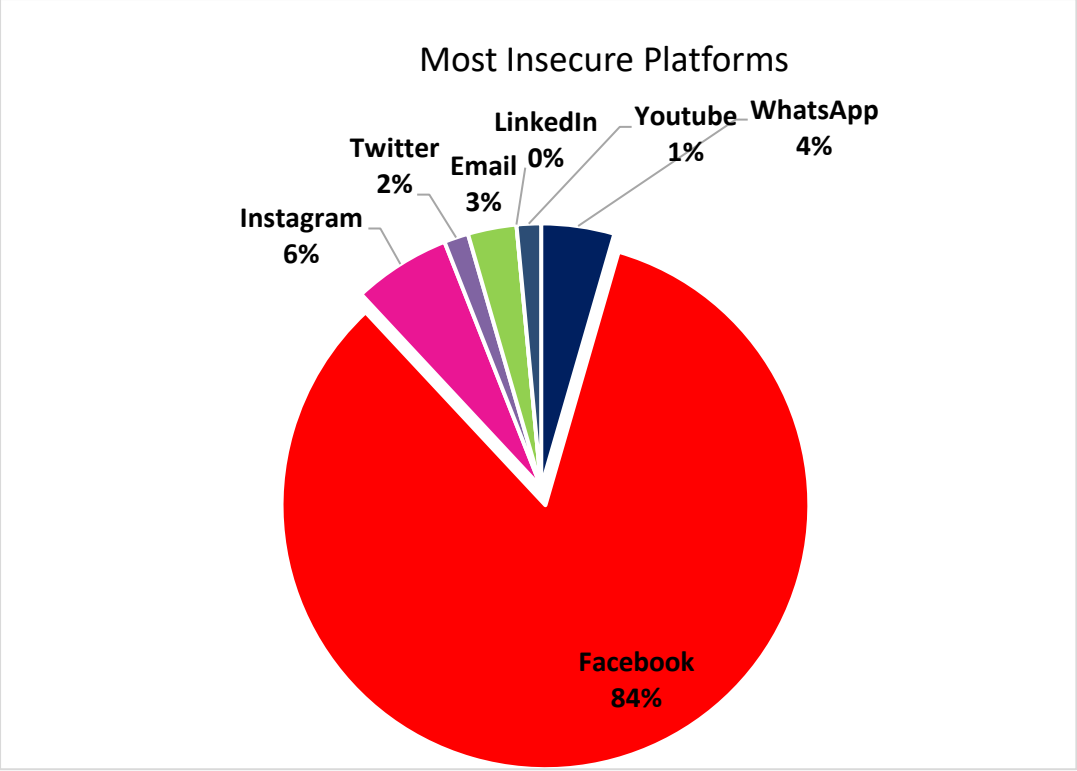


Figure 4.10: Most insecure social media platform

(*Source:* Researcher)

Table 4.3 illustrates that fake jobs were listed as the most prevalent crime in social media at 35.90%, followed by online romance scams at 16.24%, hacking at 13.68%, cyber bullying at 12.82%, cyberstalking at 11.11% and identity theft at 10.28%, based on the number of times they were listed by youth respondents.

Table 4.3: Types of crimes that result from use of social media platform

	Cyber bullying	Identity theft	Fake jobs	Hacking	Cyber stalking	Online romance scams	Total
WhatsAPP	0.85%	0.00%	0.85%	0.85%	1.71%	0.00%	4.27%
Facebook	9.40%	8.55%	29.91%	10.26%	7.69%	13.68%	79.49%
Instagram	1.71%	0.00%	2.56%	0.00%	0.00%	0.85%	5.13%
Twitter	0.85%	0.00%	0.00%	0.00%	0.00%	0.00%	0.85%
Email	0.00%	0.85%	1.71%	1.71%	0.85%	0.85%	5.98%
LinkedIn	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
YouTube	0.00%	0.85%	0.85%	0.85%	0.85%	0.85%	4.27%
Total	12.82%	10.26%	35.90%	13.68%	11.11%	16.24%	100.00%

(*Source:* Researcher)

Social media platform the youth respondents felt had the highest number of crimes was Facebook at 79.49%, followed by Email at 5.98%, Instagram at 5.13% and both WhatsApp and YouTube at 4.27%. In Facebook, fake jobs was 29.91%, online romance scams was 13.68%, hacking was 10.26%, cyber bullying was 9.40%, identity theft was 8.55% and cyberstalking was 7.69%. From results in Table 4.3, it is clear that each of the six types of crimes is highest in Facebook, lowest in Twitter and absent in LinkedIn. These findings further corroborate results by Donoghue (2017) about high level of cybercrimes associated with Facebook.

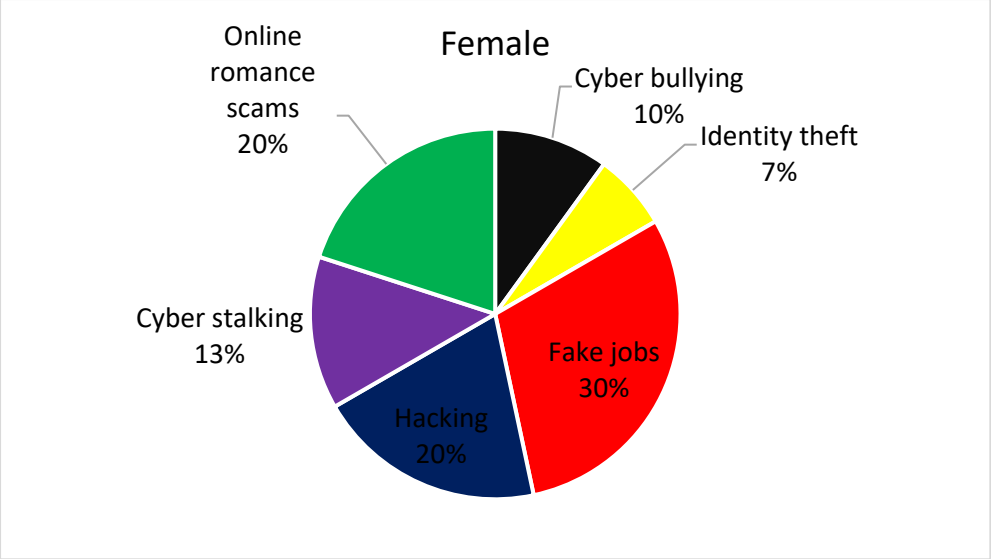


Figure 4.11: Percentage of female youth respondents who listed types of crimes

(*Source:* Researcher)

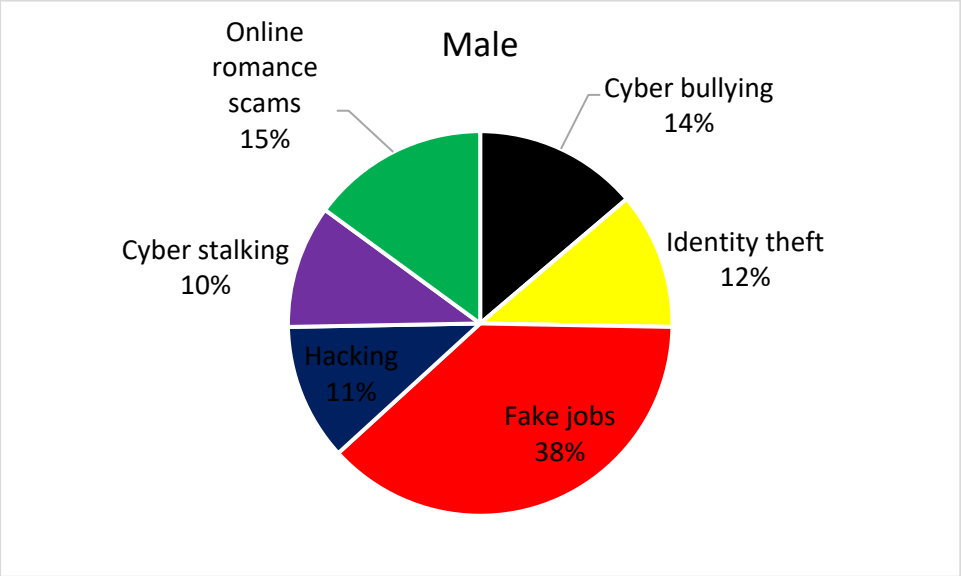


Figure 4.12: Percentage of male youth respondents who listed types of crimes

(*Source:* Researcher)

Results of further analysis of crimes that result from social media use based is presented in Figures 4.11 and 4.12. About 30% of female youth respondents had opinion that fake jobs dominated social media crimes, followed by hacking and online romance scam at 20%, cyberstalking at 13%, cyber bully 10% and identity theft at 7% (Figure 4.11). About 38% of male youth respondents similar opinion that fake jobs dominated social media crimes,

followed by cyber bullying at 14%, online romance scam at 15%, identity theft at 12%, hacking at 11% and cyberstalking 10% (Figure 4.12).

It is evident from the above analysis that at least 15% of both female and male youth respondents identify fake jobs and online romance scams as most common social media crimes. Apart from the two crimes, at least 13% of female youth respondents also felt that hacking and cyberstalking as dominant social media crimes. A similar percentage of male youth respondents felt that cyber bullying was the most dominant social media crime. The findings corroborate results of previous research carried out in Australia and Kenya on the crimes (Kwanya, Kogos, Kibe, Ogolla, & Onsare, 2021; Patel, Kannoorpatti, Shanmugam, Azam, & Yeo, 2017). The higher percentage of female than male youth respondents felt that online romance scams, hacking and cyberstalking affected them.

Figure 4.13 illustrates percentage of youth responses on social media crime type by respondent age. Generally, youth aged between 18-25 years formed the highest percentage of respondents on each social media crime, followed by those aged 26-30 years. This could be due to their number in the sample and the population studied in the current research. Social media crime with highest percentage of youth respondents that felt that it affected their social media use were 25.64% in the age group of 18-25 years, 6.84% in the age group of 26-30 years and 3.42% in the age group of 31-35. Older youth respondents in the age group 31-35 years had opinion that cyber bullying and identity theft did not result from their social media use. Youth respondents in the age groups of 18-25 and 26-30 years had opinion that all the six types of crimes could result from their use of social media, though those in the latter age group felt less affected than the former. Apart from fake jobs, most younger youth respondent felt that they were exposed to online romance (11.97% aged 18-25, 3.42% aged 26-30 years), cyber bullying (11.97% aged 18-25, 0.85% aged 26-30 years) and hacking (6.84% aged 18-25, 2.56% aged

26-30 years). Youth respondents in the age group of 31-35 years felt least exposed to the six crime types related to social media use.

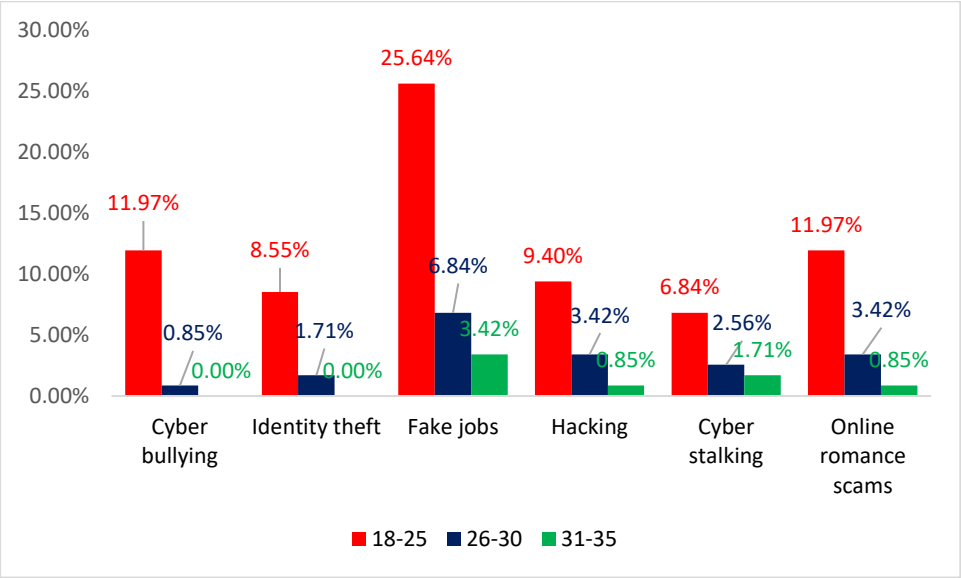


Figure 4.13: Percentage of responses on social media crime type by respondent age

(*Source:* Researcher)

The results of the current research that younger youth feel more affected by crimes resulting from their social media use corroborate findings by Oksanen and Keipi (2013) and Näsi, Oksanen, Keipi and Räsänen, (2015) who found that younger youth respondents were more likely to be exposed to cybercrime than older people.

4.3.3. Influence of Social Media on Personal Security among the Youth in Nairobi City County

Figure 4.14 illustrates the percentages of youth respondents who have been victims of social media insecurity. About 52% of the youth respondents confirmed that they had been victims, the rest had not.

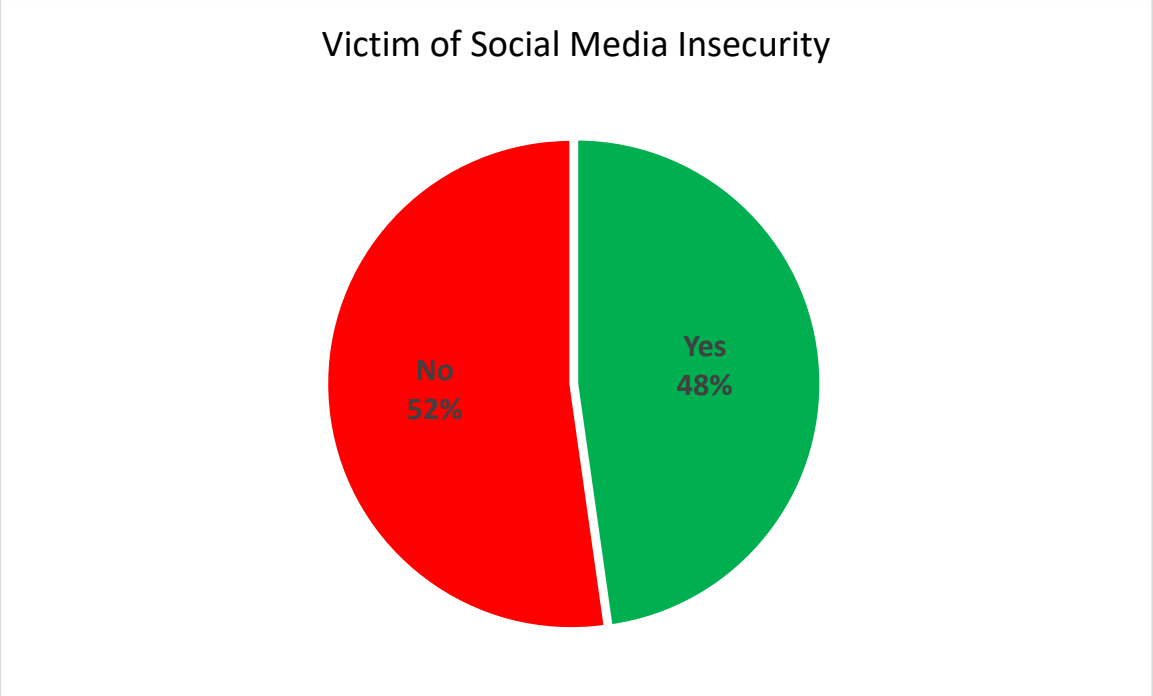


Figure 4.14: Victims of social media insecurity

(*Source:* Researcher)

Further analysis based on gender shows that of those who were victims, about 72% were male and the rest were female. These findings were different from those of Drew (2020) who found that more females than males were victims of social media crimes. The difference between these findings lie in the composition of the study population. Whereas study population in Drew (2020) was based on general community, the current research was based on PCAK membership of which female percentages were less than that of males.

A further analysis based on composition of victims within specific gender was carried out to give greater insights. About 46% of all male youth respondents were found to have been victims of social media related crimes and about 53% of all female youth respondents had also been victims. It is noteworthy that though the percentage of female youth respondents who have been victims was less than that of male in the entire sample (male 72% female 28%), their percentage based on number of females in the sample was higher that of male (female 53% of all female in sample, male 46% of all male in sample).

The results that a larger percentage of female youth respondents have been victims of crimes arising from their social media use corroborates findings by Wanjiku (2021) who found that out of 198 studied social media crimes, only two involved male victims.

Table 4.4: Feeling of safety on joining and leaving social media

Safe after joining	Safe after deactivating social media account	Frequency	Percentage
No	No	11	16.42%
No	Yes	22	32.84%
Yes	No	18	26.87%
Yes	Yes	16	23.88%
Total		67	100.00%

(*Source:* Researcher)

Results in Table 4.4 illustrates youth respondents who felt safe after joining social media were 50.75%, the rest did not feel safe after joining social media. Moreover, about 43.29% of the youth respondents did not feel safe after deactivating social media accounts. The results further show that 16.42% of youth respondents did not feel safe both after joining social media and deactivating social media account. About 32.84% of the respondents did not feel safe after joining social media but felt safe after deactivating social media account. About 26.87% of the youth respondents felt safe after joining social media but did not feel safe after deactivating social media account. About 23.88% felt safe both after joining and after deactivating social media account.

From the results, it was noted that about 76.12% of all the youth respondents did not feel safe either at joining or at deactivating social media account. This confirms findings in literature that social media influences personal security corroborate literature that speedy diffusion and adoption of various forms of social media platforms "*has exposed the Kenyan public to unprecedented individual security threats*" (Okuku, Renaud, & Valeriano, 2015). The finding that social media poses security threats to persons have been established in the findings of this research and also confirm the findings of Spangler (2019) that social media usage has adverse

effects and can lead to lose of privacy. The results of this research indicate that social media has security risks that continue even after deactivation of account and this confirms findings of Rathore, Sharma, Loia, Jeong and Park (2017) that showed that content associated with social media can still risk security even if the link has been deleted.

4.5. Findings from Law Enforcement Officers

4.5.1. Common Social Media Crimes Reported

Results in Table 4.5 illustrate common social media crimes. The about 29.36% of the law enforcement informants had opinion that cyber bullying is common, 9.17% had opinion it was hacking and 7.34% had opinion that fraud was common. Cyber stalking and pornography were identified by 3.67% of the law enforcement informants. About 2.75% of the law enforcement informants had opinion that defamation, harassment, hate speech, kidnapping, money laundering, obtaining by false pretence, phishing and online threats were commonly reported social media crimes. The lowest percentage of law enforcement informants believed that the commonly reported social media crimes were body shaming, blackmailing, character assassination, copyright infringement, corruption, drug abuse, extortion, forgery, gender violence crimes, identity theft, illegal trade, incitement, insults, libel, online romance scams, slander, terrorism and vacation robberies

Table 4.5: Common social media crimes reported

Cyber crime	Frequency of identification	Percentage
Cyber bullying	32	29.36%
Hacking	10	9.17%
Fraud	8	7.34%
Impersonation	5	4.59%
Cyber stalking	4	3.67%
Pornography	4	3.67%
Defamation	3	2.75%
Harassment	3	2.75%
Hate speech	3	2.75%
Kidnapping	3	2.75%
Money laundering	3	2.75%
Obtaining by false pretence	3	2.75%
Phishing	3	2.75%
Threats	3	2.75%
Radicalization	2	1.83%
Sexual harrassment	2	1.83%
Body Shaming	1	0.92%
Blackmailing	1	0.92%
Character assasination	1	0.92%
Copyright infringement	1	0.92%
Corruption	1	0.92%
Drug abuse	1	0.92%
Extortion	1	0.92%
Forgery	1	0.92%
Gender violence crimes	1	0.92%
Identity theft	1	0.92%
Illegal trade	1	0.92%
Incitement	1	0.92%
Insults	1	0.92%
Libel	1	0.92%
Online romance scams	1	0.92%
Slander	1	0.92%
Terrorism.	1	0.92%
Vacation Robberies	1	0.92%
Total	109	100.00%

The results that highest percentage of law enforcement informants believed that were commonly reported cybercrimes in social media corroborate findings of Alasa (2019) who

carried out research in Nigeria and found that cyberstalking, child pornography, computer-related fraud and impersonation dominate reported cybercrimes. The results of this research also confirm findings of Magufuli (2019) in his PhD dissertation focused on social media use in Dar-es-Salaam in Tanzania and found that fraud, forgery, identity theft, phishing, pornography, hacking, libel and fake news dominate common cybercrimes reported to law enforcement. The results also corroborate findings of Kiprugut (2017) who carried out research on social media use among young people in Kenya and found out that the commonly reported cybercrime included fraud, cyberstalking, child pornography and unauthorized access.

4.5.2. Average Age of Social Media Victims

Law enforcement informants responses on average age of social media victims were as illustrated in Table 4.6. About 43.55% of law enforcement informants had opinion that social media victims were age of at least 18 years. About 14.52% of the respondents had opinion that the average age was 20 years or more. Law enforcement informants who believed the age of social media victims was 25 years or more and those who had opinion it was 35 years or more were 6.45% in each case.

Table 4.6: Average age of social media victims

	Frequency	Percentages
16 and above	3	4.84%
18 and above	27	43.55%
20 and above	9	14.52%
25 and above	4	6.45%
30 and above	2	3.23%
35 and above	4	6.45%
40 and above	2	3.23%
All ages	1	1.61%
No clear response	10	16.13%
Total	62	100.00%

About 3.23% of the respondents believed that the victims were of age of at least 30 years and a similar percentage of the respondents believed the age was at least 40 years. About 1.61% had opinion that the victims were of all ages. It was estimated that 16.13% of the law enforcement informant did not give clear response on average age. Therefore, highest percentage of law enforcement informants had opinion that those aged 18 years and above were common victims which confirm findings of Munyua (2013) that victims were mostly aged between 18 and 32 and were predominantly female.

4.5.3. Victim Gender

Results in Figure 4.15 illustrates that law enforcement informants had opinion on victims of social media crimes. About 68% of the law enforcement informants believed that both males and females were victims. About 31% believed that most victims were females and about 1% believed the that most victims were male.

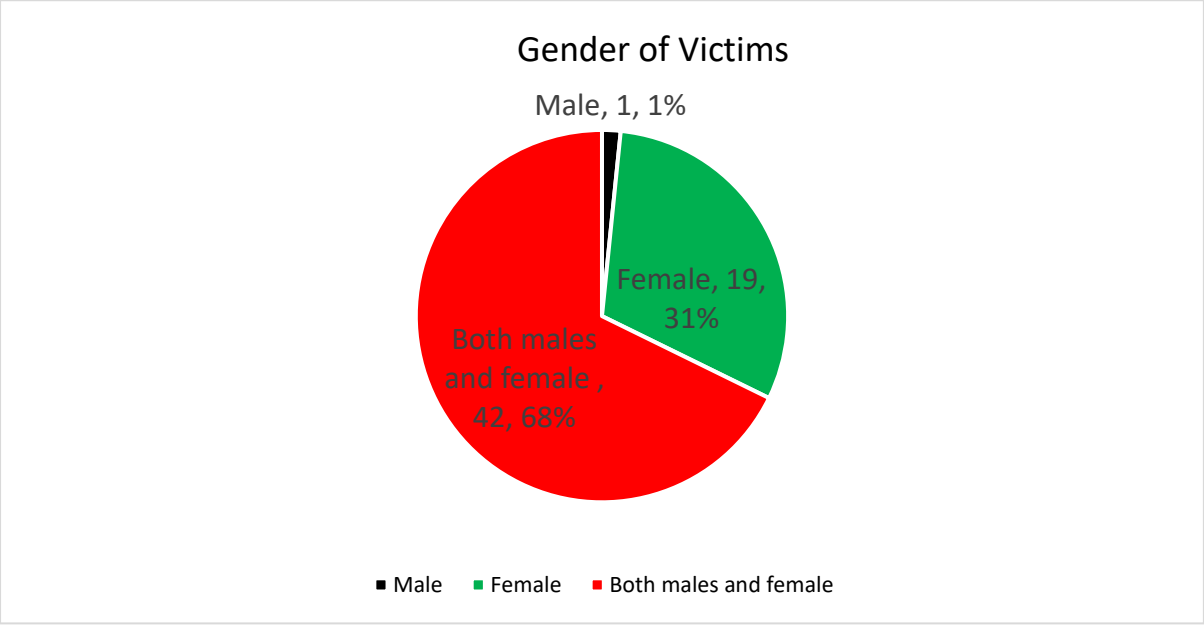


Figure 4.15: Gender of victims of social media crimes

(*Source:* Researcher)

Law enforcement informants who had opinion that both gender were victims gave reasons that both use social media and criminals do not discriminate. Other respondents argued that factors contributing to victimology know no gender. The informants who had opinion that females were more predisposed than men noted that young females go by the trending habits which renders them vulnerable since most of them easily trust strangers and give too much information. The informants stated that mostly female are prone to sharing their personal data online than male and that they trust strangers easily. They noted that the suspects will take nude pictures of young girls and threaten to expose by sending to social media groups where the victim is a member. The informants cited stereotyping any advertisement marketing of products the face or pictures of women are used making are susceptible to feeling the effects of that.

The opinion of the law enforcement informants that women were more vulnerable to cybercrime corroborate findings of Jaishankar (2020) who noted that apart from women being more vulnerable to be a victims, the impact of victimization is more on them compared to men. The results also confirm findings of Munyua (2013) and Wanjiku (2021) that victims of cybercrimes such as cyberstalking are predominantly female. The opinion of the law enforcement informants that both gender are equally vulnerable to cybercrime corroborate findings in previous survey that the share of men falling victim to cybercrime was just as large as that of women (Central Bureau of Statistics, 2019).

4.5.4. Time Spent on Social Media and Predisposition

Results in Figure 4.16 illustrates that about 79% of the law enforcement informants agreed that time spent on social media has relationship with predisposition to social media crimes. This corroborates findings in literature that time spent online increases the possibility of exposure to risks and pathological tendencies such as cyberbullying (Hay & Ray, 2020; Throuvala, Griffiths, Rennoldson, & Kuss, 2021). The rest of the law enforcement informants did not agree.

The respondents who did not agree cited various reasons including nature of activities one is involved with in social media, socioeconomic and political factors at a specific stage of life, the type of audience one entertains and type of social media one is engaged in. Other informants argued that so many people are active in social media and not victims. They noted that spending more time on social media gives one exposure and knowledge to know modus operandi of the perpetrators and this one becomes aware of the vulnerabilities of social media. It was also noted that one can become a victim of cybercrime without spending more time on social media.

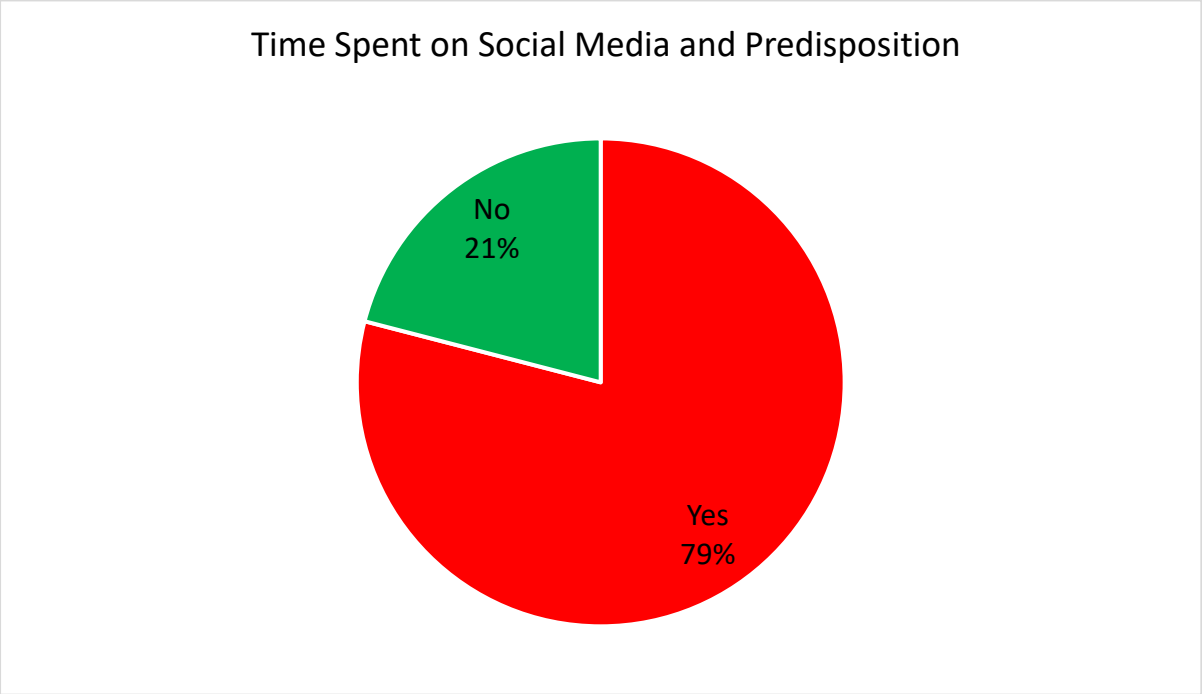


Figure 4.16: Time spent on social media and predisposition to crime

(*Source:* Researcher)

4.5.5. Existing Laws in Curbing Social Media Crimes

The law enforcement informants identified the following laws that address social media crimes:-

i. Anti-Corruption and Economic Crimes Act
ii. Computer Misuse and Cybercrime act No. 5 of 2018
iii. Data Protection Act No. 24 of 2019

iv. Kenya Information and Communications act 2015.
v. National Cohesion and Integration Act (NCIC) 2008
vi. Penal Code CAP 63 Laws of Kenya
vii. Prevention of Fraud (Investments) Act 1977
viii. Prevention of Terrorism Act No. 30 of 2012
ix. Proceeds of Crime and Anti-Money Laundering Act No. 9 of 2009
x. The Constitution of Kenya 2020
xi. The Sexual Offences Act. No 3 of 2006

The laws identified by the law enforcement informants are the main ones applicable in prosecuting cybercrimes. However, they are not exhaustive and fail to take account of international law. Acts of parliament as well as regulations that are passed from time to time also address cybercrimes. One key law now applicable in addressing cybercrime is the Security Laws (Amendment) Act, No 19 of 2014 read together with High Court declarations and orders in Security Law Amendment Act Ruling dated 23rd February, 2015.

4.5.6. Penalties for Social Media Offences

Results in Table 4.7 illustrate the penalties that law enforcement informant associated with social media offences. About 33.87% of the law enforcement informants stated that imprisonment was the most common penalty while about 29.03% stated that it was either imprisonment, fines or both. About 19.35% of the informants had opinion that fines were most common penalties. The rest of the informants were either not sure or gave irrelevant responses. The findings in the current research confirm literature that prison penalties and fines are most often sentenced to perpetrators of social media crimes (Naro, et al., 2020).

Table 4.7: Penalties for social media offences

Penalty	Frequency	Percentage
Imprisonment	21	33.87%
Imprisonment, Fines	18	29.03%
Fines	12	19.35%
Not sure/ no response	11	17.74%
Total	62	100.00%

(*Source:* Researcher)

4.5.7. Challenges Encountered in Investigation and Prosecution of Social Media Crimes

Table 4.8 illustrates law enforcement informants' responses on challenges facing investigation and prosecution of social media. The challenges were grouped into tracking, capacity, technological and legal challenges. Tracking challenges believed to be as a result of fake social media accounts which made it difficult to find victims and perpetrators. Little international cooperation in tracking especially where cross-border crimes were involved was also identified as major challenges. The informants also noted that most social media crimes go unreported and therefore no investigation or prosecution is done. The findings that tracking is a major challenge in investigating and prosecuting social media crimes corroborate literature that shows that offensive content detection and tracking of perpetrators and victims in social media is a multilingual, multi-level, multi-class classification problem due to use of various languages (Modha, Mandl, Majumder, & Patel, 2020; Uldam, 2018).

Table 4.8: Challenges in investigation and prosecution of social media crimes

Tracking challenges	Difficulties in finding the victims Challenges on public and private sector partnerships cooperation in tracking Confidentiality of information, shame hence people rarely report or want to publicly give information or evidence Electronic evidence gathering due to transnational involvement of service providers Fake social media accounts Lack of cooperation from the tech giants providing the services like Facebook, Twitter and so on. Little international cross border cooperation in tracking

	Most cases go unreported. Poor reporting by victims of cybercrimes. The need to track down sophisticated users who commit unlawful acts on the Internet while hiding their identities
Capacity challenges	Inadequate capacity for gathering and keeping of proper evidence to be used in the law courts for conviction Insufficient technical know-how to investigate and resolve cyber crimes Lack of capacity for law enforcement officers to prosecute the crimes Lack of capacity to enable close coordination among law enforcement agencies Lack of or inadequacy of proper equipment to trace , capture or outline the evidence needed Lack of resources Lack of trained and well-equipped personnel to gather evidence, investigate, and prosecute these cases. Lack proper systems in place to address and steer cyber security policies Limited investigation knowledge due to continuous change of technology
Technological Challenges	Technological capabilities to investigate and identify identities of the criminals since most of them use profile identities of other persons. Technological enhancement makes it difficult to arrest and prosecute a given suspect Fast changing social media technologies Technology adoption challenges in law enforcement
Legal challenges	Challenge to prove cybercrime case beyond reasonable doubt Court are lenient on offenders. Criminals destroy evidences Cyber space is a big endless space- ungoverned- it's difficult to successfully track cases Gaps in applicable laws, lack of capacity in investigations, gaps in understanding prosecution procedure and evidence presentation. Getting witnesses, and evidence because it revolves around gadgets Getting court orders to access vital information which is then used in prosecution is a challenge Investigations tend to take long Lack of audit trail and proper legislation relating to social media Lack of concrete evidence as most of the perpetrators are smart in eliminating traces of evidence Lack of mutual legal agreement with host countries Lack of sufficient evidence

	Many loopholes, because the existing laws are still have gaps. Minimal sentences which allows for recidivism Poor enforcement of the ICT laws. Slow litigation procedure- leading to delayed or even non conviction The law on computer and cybercrime is neither clear nor specific The laws bordering on cybercrime have not been fully implemented.

Law enforcement informants also identified capacity challenges such as lack of capacity for law enforcement officers to prosecute the crimes and that to enable close coordination among law enforcement agencies. Other capacity challenges identified by the informants included lack of or inadequacy of proper equipment to trace , capture or outline the evidence needed, lack of resources and lack of trained and well-equipped personnel to gather evidence, investigate, and prosecute these cases. Further, the law enforcement informants had opinion that lack proper systems in place to address and steer cyber security policies was a capacity challenge as well as limited investigation knowledge due to continuous change of technology. The findings that capacity challenges affect investigation and prosecution of social media crimes corroborate findings of Clarke (2018) who identified capacity challenges as obstacles of investigating and prosecuting such cases within and between nations. To address capacity challenges, the informants suggested cooperation among actors in line with recommendations of Seelinger (2020).

Technological challenge identified by the law enforcement informants included inadequate technological capabilities to investigate and identify identities of the criminals since most of them use profile identities of other persons. The informants also felt that fast technological enhancements make it difficult to arrest and prosecute a social media suspects. Other challenges identified were fast changing social media technologies that require law enforcement to cope with and technology adoption challenges within law enforcement

organizations. The findings confirm literature that unpreparedness to deal with new technologies is a major challenge in investigating and prosecuting social media crimes (Caianiello, 2019; Georgiou, 2017)

CHAPTER FIVE

SUMMARY OF FINDINGS, CONCLUSIONS AND RECOMMENDATIONS

5.1. Introduction

This chapter presents summary of findings on forms of social media, social media crimes, influence of social media on personal security and challenges facing investigation and prosecution of social media crimes. It also presents conclusions and general recommendations, policy recommendations and suggestions for future research.

5.2. Summary of Findings

5.2.1. Forms of Social Media Among the Youth In Nairobi City County

The results of the current research show that youth mostly prefer WhatsApp over other social media platforms possibly because it provides simple, personal and real time messaging without any cost other than their internet data already in their smart phones (Jisha & Jebakumar, 2014; Udenze, 2017). Percentage usage of WhatsApp was 84% in the current research compared to 89% in literature (SIMElab Africa, 2019). From the results, the most preferred social media platforms by both gender was WhatsApp and Twitter. It was also found in the current research that older youth in the age group of 31-35 years did not prefer Facebook, Instagram, Twitter, Email and LinkedIn but preferred WhatsApp. This was possibly be due to privacy of WhatsApp and its convenience in communicating with friends and group members. WhatsApp, Facebook, Twitter, Instagram and Emails were most preferred by younger youth in the age bracket of 18-25 years. Email and LinkedIn were preferred by students. Facebook and Twitter were preferred equally among job seekers and employed youth respondents. Instagram was also mostly used in equal measure of 33.33% among each of the groups. About 39.29% of youth who mostly used WhatsApp were students, 35.71% were job seekers while 25% were employed.

5.2.3. Crimes that Result from Social Media Use among the Youths in Nairobi City County

The findings of this research show that about 84% of youth respondents had opinion that Facebook was most insecure. Fake jobs were listed as the most prevalent crime in social media by youth respondents at 35.90% of all the social media crimes listings in this research. It was followed by online romance scams at 16.24%, hacking at 13.68%, cyber bullying at 12.82%, cyberstalking at 11.11% and identity theft at 10.28%, based on the number of times they were listed by youth respondents. The youth respondents felt that social media platform that had the highest number of crimes was Facebook at 79.49%, followed by Email at 5.98%, Instagram at 5.13% and both WhatsApp and YouTube at 4.27%. In Facebook, fake jobs was listed as most common at 29.91%, online romance scams was 13.68%, hacking was 10.26%, cyber bullying was 9.40%, identity theft was 8.55% and cyberstalking was 7.69%. About 30% of female youth respondents had opinion that fake jobs dominated social media crimes, followed by hacking and online romance scam at 20%, cyberstalking at 13%, cyber bully 10% and identity theft at 7%

About 25.64% of youth respondents that felt social media crimes affected them were in the age group of 18-25 years, 6.84% were in the age group of 26-30 years and 3.42% were in the age group of 31-35. Older youth respondents in the age group 31-35 years had opinion that cyber bullying and identity theft did not result from their social media use. Youth respondents in the age groups of 18-25 and 26-30 years had opinion that all the six types of crimes could result from their use of social media, though those in the latter age group felt less affected than the former. The results of the current research that younger youth feel more affected by crimes resulting from their social media use corroborate findings by Oksanen and Keipi (2013) and Näsi, Oksanen, Keipi and Räsänen, (2015).

5.2.3. Influence of Social Media on Personal Security among the Youth in Nairobi City County

The study found that about 52% of the youth respondents confirmed that they had been victims. Also about 72% of those who confirmed they had been victims were male and the rest were female. Of all the male youth respondents about 46% were found to have been victims of social media related crimes and about 53% of all female youth respondents had also been victims. The results corroborate findings by Wanjiku (2021). Youth respondents who felt safe after joining social media were 50.75%, the rest did not feel safe after joining social media. Moreover, about 43.29% of the youth respondents did not feel safe after deactivating social media accounts. The results further show that 16.42% of youth respondents did not feel safe both after joining social media and deactivating social media account. About 32.84% of the respondents did not feel safe after joining social media but felt safe after deactivating social media account. Generally, about 76.12% of all the youth respondents did not feel safe either at joining or at deactivating social media account, findings that corroborate Spangler (2019).

5.2.4. Challenges Facing Investigation and Prosecution of Social Media Crimes Among the Youth in Nairobi City County

Challenges facing investigation and prosecution of social media crimes were found in the current research to be tracking, capacity, technological and legal challenges. Tracking challenges were believed to be as a result of fake social media accounts, little international cooperation in tracking especially where cross-border crimes were involved. Capacity challenges identified included lack of capacity for law enforcement officers to prosecute the crimes and that to enable close coordination among law enforcement agencies. Other capacity challenges identified by the informants included lack of or inadequacy of proper equipment to trace , capture or outline the evidence needed, lack of resources and lack of trained and well-

equipped personnel to gather evidence, investigate, and prosecute these cases. Technological challenge identified by the law enforcement informants included inadequate technological capabilities to investigate and identify identities of the criminals since most of them use profile identities of other persons. The informants also felt that fast technological enhancements make it difficult to arrest and prosecute a social media suspects.

5.3. Conclusions

Forms of social media that youth mostly prefer is WhatsApp over other social media platforms. The most preferred social media platforms by both gender was WhatsApp and Twitter. Youth in the age group of 31-35 years did not prefer Facebook, Instagram, Twitter, Email and LinkedIn but preferred WhatsApp. WhatsApp, Facebook, Twitter, Instagram and Emails were most preferred by younger youth in the age bracket of 18-25 years. Email and LinkedIn were preferred by students. Facebook and Twitter were preferred equally among job seekers and employed youth respondents.

The findings of this research show that about 84% of youth respondents in Nairobi City County had opinion that Facebook was most insecure. The findings of this research show that about 84% of youth respondents had opinion that Facebook was most insecure. Fake jobs were listed as the most prevalent crime in social media by youth respondents at 35.90% of all the social media crimes listings in this research. The youth respondents felt that social media platform that had the highest number of crimes was Facebook. In Facebook, fake jobs was listed as most common at 29.91%, online romance scams was 13.68%, hacking was 10.26%, cyber bullying was 9.40%, identity theft was 8.55% and cyberstalking was 7.69%. Older youth respondents in the age group 31-35 years had opinion that cyber bullying and identity theft did not result from their social media use. The results of the current research that younger youth feel more affected by crimes.

Social media was found to have influence on personal security among the youth in Nairobi City County. The study found that about 52% of the youth respondents confirmed that they had been victims. Youth respondents who felt safe after joining social media were 50.75%, the rest did not feel safe after joining social media. Moreover, about 43.29% of the youth respondents did not feel safe after deactivating social media accounts. It was concluded that insecurity arising from social media use was likely to continue beyond social media account deactivation.

Challenges facing the investigation and prosecution of social media crimes among the youth in Nairobi City County were found to range from tracking, capacity, technological and legal challenges. Tracking challenges were found to result from fake social media accounts and problems of international cooperation in investigations and prosecution, among other challenges. Capacity challenges were found to include lack of capacity to prosecute the crimes, inadequate coordination among law enforcement agencies, lack of or inadequacy of proper equipment, lack of resources and lack of trained and well-equipped personnel to gather evidence, investigate, and prosecute social media crimes.

5.4. Recommendations

It is recommended that for tracking of social media criminals and victims to be improved, there should be awareness creation to the youth to come out and identify possible accounts, interactions and persons likely to be suspects. Victims should not fear reporting to law enforcement agencies. Public and private sector partnerships and cooperation in tracking of suspects of social media crimes should be improved. There should be more cooperation between law enforcement agencies and social media service providers even across national borders to identify criminals. Mechanisms should be put in place to identify, monitor and deactivate fake social media accounts. There should cooperation between law enforcement

agencies and the society and police-public initiatives that aim to address social media crimes should be put in place.

Capacity of law enforcement agencies to prevent, identify and prosecute social media crimes should be improved. Specifically, capacity for gathering and keeping of proper evidence to be used in the law courts for conviction should be enhanced. Technical know-how of law enforcement officers to investigate and resolve cyber crimes should be improved. There should be better capacity of law enforcement agencies to have close coordination and sharing of relevant information to improve cyberspace policing. Law enforcement agencies need to be properly equipped to trace, capture or outline the evidence needed. It is further recommended that adequate resources such as finances should be given to law enforcement agencies to support their operations on social media. Personnel involved in law enforcement should be trained to gather evidences, investigate, and prosecute these cases. Necessary systems should be put in place to address and steer cyber security policies and to boost investigation knowledge to enable law enforcement to adapt to continuous change of technology.

Technological capabilities of law enforcement agencies should be enhanced and made to keep with the fast changing social media technologies. Specifically, technologies that enable law enforcement to investigate and identify social media criminals should be adopted and made to be in tandem with advances in technology. There should be organizational support of social media policing and presence since the modern society is mainly digital and criminals have also improved their strategies.

Legal framework for investigating and prosecuting cyber crimes should be improved and should keep up with the every changing technologies. Specifically, there should be a legal framework enabling proof of cybercrime cases based on new technologies. Courts should not be seen to be too lenient to cyber criminals as a result of unreasonable requirements. There should be clear legal framework for social media governance. Investigations and litigation

process for cybercrimes should not take long. Proper framework should be put in place to ensure audit trails and evidences are not tampered with. There should be a binding agreements among countries to provide a framework for investigating and prosecuting cross-border social media crimes. Available laws and regulations on cybercrime should be well implemented and proper one be put in place where there are gaps.

5.5. Policy Recommendations

There should be clear policies on social media. Currently, Kenya has ICT policies and there is no specific policy addressing social media. Specific policies on social media and social media crimes should be put in place. Better policies on investigation and prosecution of social media crimes should be put in place to support implementation of laws addressing social media crimes. Regional and international policies on addressing cross-border social media crimes should also be put in place. There should be a law enforcement unit dedicated to social media and with clear policy guidelines on its operations and powers.

5.6 Recommendations on Future Research

Future research can focus on the issue of social media and personal security influences on youth and its spatial dispersion. Such dispersions should be based on real social media crime incidences by type time, age, gender and location to give insights on how policing can be enhanced in response to such dispersion and temporal diffusion of such crimes especially on mobile platforms.

REFERENCES

Abaido, G. M. (2020). Cyberbullying on social media platforms among university students in the United Arab Emirates. *International Journal of Adolescence and Youth*, *25*(1), 407–420. https://doi.org/10.1080/02673843.2019.1669059

Ackerman, S., & Schutte, K. (2015). *Social Media as a Vector for Cyber Crime*.

Aissani, R., & Dheyab Abdullah, A. (2018). Motives for the use of Twitter by Arab youth. *Communication Today*, *9*(1).

Aizenkot, D. (2018). *Cyberbullying in WhatsApp Classroom Groups among Children and Adolescents: Exposure and Victimization*. *10*, 1–10.

Akakandelwa, A., & Walubita, G. (2017). Students' social media use and its perceived impact on their social life: A case study of the University of Zambia. *The International Journal of Multi-Disciplinary Research*, (October), 1–14. Retrieved from https://www.researchgate.net/publication/328389136

Al-Amin, M., Nafi, S. M., & Amin, A. (2019). *Use of social media for job search and application: A perspective from the job seekers in Bangladesh*. *July*. Retrieved from www.discoveryjournals.org

Alasa, A. (2019). *A Legal Analysis of Cybercrimes and Cybertorts: Lessons for Nigeria.* Available at SSRN 3560905.

Alava, S., Frau-Meigs, D., & Hassan, G. (2017). *Youth and violent extremism on social media: mapping the research.* UNESCO Publishing.

Almarabeh, H. (2019). The Impact of Cyber Threats on Social Networking Sites. *International Journal of Advanced Research in Computer Science*, *10*(2), 1–9. https://doi.org/10.26483/ijarcs.v10i2.6384

AlNajjar, A. (2019). Abolish censorship and adopt critical media literacy: A proactive approach to media and youth in the Middle East. *Journal of Media Literacy Education, 11*(3), 73-84.

Al-Shami, A. M. (2021). *Yemen: Unsettled Media for an Unsettled Country*. Open Book Publishers.

Arigo, D., Pagoto, S., Carter-Harris, L., Lillie, S. E., & Nebeker, C. (2018). Using social media for health research: Methodological and ethical considerations for recruitment and intervention delivery. *Digital Health*, *4*, 2055207618771757.

Asongu, S. A., Uduji, J. I., & Okolo-Obasi, E. N. (2019). Homicide and social media: Global empirical evidence. *Technology in Society*, *59*, 101188.

Bake. (2018). *State of the Internet in Kenya 2017*. 33. Retrieved from https://www.ifree.co.ke/wp-content/uploads/2018/02/State-of-the-Internet-in-Kenya-report-2017.pdf

Bichir, V. (2011). Social and economic impact of internet social networks: Survey on Facebook network. *International Conference Modern Approaches in Organisational Management and Economy . 5*, pp. 74-77. Bucharest, Romania: Faculty of Management, Academy of Economic Studies.

Bradshaw, S., Neudert, L. M., & Howard, P. N. (2018). *Government responses to malicious use of social media.* NATO StratCom Centre of Excellence, Riga, Working Paper.

Brainard, A. (2018). A Content Analysis of Crimes Posted on Social Media Platforms. *82-Elon Journal of Undergraduate Research in Communications*, *9*(1), 82–94.

Byrne, E., Vessey, J. A., & Pfeifer, L. (2018). Cyberbullying and social media: Information and interventions for school nurses working with victims, students, and families. *The Journal of School Nursing, 34*(1), 38-50.

Caianiello, M. (2019). Criminal process faced with the challenges of scientific and technological development. *European Journal of Crime, Criminal Law and Criminal Justice, 27*(4), 267-291.

Calbalhin, J. P. (2018). Facebook User's Data Security and Awareness: A Literature Review. *Journal of Academic Research*, *2*(June 2018), 1–13.

Center, P. R. (2018). *Social media use continues to rise in developing countries but plateaus across developed ones: Digital divides remain, both within and across countries*. *June*, 1–46. Retrieved from https://assets.pewresearch.org/wp-content/uploads/sites/2/2018/06/15135408/Pew-Research-Center_Global-Tech-Social-Media-Use_2018.06.19.pdf

Central Bureau of Statistics. (2019). *Digital Security & Crime 2018.*

Chege, S. (2019). *An Assessment of Social Media Usage among TVET Students in Kiambu County , Kenya*. *January*. https://doi.org/10.13140/RG.2.2.29830.83526

Chytiri, A. P. (2015). *Hotel Recruitment and Selection Practices: The case of Greek Hotel Units/Chains Vs Foreign Hotel Units/Chains in Greece.* (Doctoral dissertation, University of Kent).

Cibra, V. (2017). *Social Media and Terrorist Organizations: Observing Success of Recruitment Through Social Media*. *February*. https://doi.org/10.13140/RG.2.2.21311.05283

Clarke, C. P. (2018). *Investigating and Prosecuting Cases of the Nexus between Organised Crime and Terrorism:: Best Practices and Lessons Learned for Practitioners.* International Centre for Counter-Terrorism .

Costa, C., & Murphy, M. (2019). EU digital media policies and education: The challenge of a digital agenda for Europe. In *Education and Public Policy in the European Union* (pp. 149 - 164). Palgrave Macmillan, Cham.

Cross, C., Dragiewicz, M., & Richards, K. (2018). Understanding romance fraud: Insights from domestic violence research. *The British Journal of Criminology*, *58*(6), 1303–1322.

Crump, J. (2011). What Are the Police Doing on Twitter? Social Media, the Police and the Public. *Policy and Internet, 3*(4).

Darden, J. T. (2019). *Tackling Terrorists' Exploitation of Youth*.

De Jong, K. (2019). *Detecting the online romance scam: Recognising images used in fraudulent dating profiles*.

Dhami, A., Aggarwal, N., Chakraborty, T. K., Singh, B. P., & Minj, J. (2013). Impact of trust, security and privacy concerns in social networking: An exploratory study to understand the pattern of information revelation in Facebook. *2013 3rd IEEE International Advance Computing Conference (IACC)*, 465–469.

Dillman, D. A., & Smyth, J. D. (2007). Design effects in the transition to web-based surveys. *Amrican Journal of Preventive Medicine, 32*(5), S90–S96.

Donoghue, B. (2017). *Risks: Hacking, Identity Theft and Burglary that are associated with students (aged 18-24) in sharing personal data through Social Media Applications.* (Doctoral dissertation, Cardiff Metropolitan University).

Drew, J. M. (2020). A study of cybercrime victimisation and prevention: exploring the use of online crime prevention behaviours and strategies. *Journal of Criminological Research, Policy and Practice*.

Dubord, P. (2008). *Investigating cybercrime*. *Handbook of Digital and Mutlimedia Forensic Evidence*. https://doi.org/10.1007/978-1-59745-577-0_6

Elsaesser, C. M., Patton, D. U., Kelley, A., Santiago, J., & Clarke, A. (2021). Avoiding fights on social media: Strategies youth leverage to navigate conflict in a digital era. *Journal of Community Psychology, 49*(3), 806–821.

Endeley, R. E. (2018). End-to-end encryption in messaging services and national security—case of WhatsApp messenger. *Journal of Information Security, 90*(01), 95.

Faria, J. (2021, November 26). *Main cyber crimes reported in Kenya 2020*. Retrieved from Statista: https://www.statista.com/statistics/1278773/number-of-online-crimes-reported-in-kenya-by-type/

Feuls, M., Fieseler, C., & Suphan, A. (2014). A social net? Internet and social media use during unemployment. *Work, employment and society*, *28*(4), 551-570.

Friese, S. (2019). *Qualitative data analysis with ATLAS. ti*. Sage.

Gachau, J. (2018). *The role of social media in participatory democracy*.

Gasper, D., & Gomez, O. (2015). Human Security Thinking in Practice—' Personal Security ', ' Citizen Security ', Comprehensive Mappings Professor Des Gasper International Institute of Social Studies , The Hague Erasmus University Rotterdam , The Netherlands Dr. Oscar A. Gómez Gradua. *Contemporary Politics*.

George, J., Sabu, A. M., & Jamir, A. (2020). A study on youth perception about social networking websites violating basic human privacy rights. *IJRAR-International Journal of Research and Analytical Reviews (IJRAR), 7*(1), 425-429.

Georgiou, L. (2017). *Social media and open trial: an emerging conflict or an opportunity?* Edinburgh Research Archive.

Ghai, S., Magis-Weinberg, L., Stoilova, M., Livingstone, S., & Orben, A. (2022). Social Media and Adolescent Well-being in the Global South. *Current Opinion in Psychology*, 101318.

Ghazinour, K., & Ponchak, J. (2017). Hidden Privacy Risks in Sharing Pictures on Social Media. *Procedia Computer Science*, *113*, 267–272. https://doi.org/10.1016/j.procs.2017.08.367

Gierszewski, J. (2017). Personal Security within the Human Security Paradigm. *Security Dimensions. International and National Studies*, *23*, 51–66. https://doi.org/10.24356/SD/23/2

Gottfried, J., & Shearer, E. (2019). *News use across social media platforms 2016*.

Gupta, S. S., Thakral, A., & Choudhury, T. (2018). *Social media security analysis of threats and security measures*. 115–120.

Harding, J. (2018). *Qualitative data analysis: From start to finish*. Sage.

Hay, C., & Ray, K. (2020). *General strain theory and cybercrime. The Palgrave handbook of international cybercrime and cyberdeviance.* 583-600.

Heale, R., & Twycross, A. (2015). Validity and reliability in quantitative studies. *Evidence-Based Nursing*, *18*(3), 66–67. https://doi.org/10.1136/eb-2015-102129

Henson, B., Reyns, B. W., & Fisher, B. S. (2016). Cybercrime Victimization. *The Wiley Handbook on the Psychology of Violence*, *January*, 553–570. https://doi.org/10.1002/9781118303092.ch28

Herrero-Diz, P., & Ramos-Serrano, M. (2018). Breaking stereotypes online: Young activists' use of the internet for social well-being. *Catalan Journal of Communication & Cultural Studies*, *10*(1), 99-114.

Hruska, J., & Maresova, P. (2020). Use of Social Media Platforms among Adults in the United States—Behavior on Social Media. *Societies*, *10*(1), 27. https://doi.org/10.3390/soc10010027

Hu, X., & Lovrich, N. P. (2019). Social media and the police: A study of organizational characteristics associated with the use of social media. *Policing*, *42*(4), 654–670. https://doi.org/10.1108/PIJPSM-09-2018-0139

Hufnagel, S., Moiseienko, A., Leukfeldt, R., & Kleemans, E. R. (Edward). (2019). Cybercrime, money mules and situational crime prevention. *Criminal Networks and Law Enforcement*, *June*, 75–89. https://doi.org/10.4324/9781351176194-5

Intahchomphoo, C. (2018). Social media and youth suicide: A systematic review. *26th European Conference on Information Systems: Beyond Digitization - Facets of Socio-Technical Change, ECIS 2018*, *October*.

Irshad, S., & Soomro, T. R. (2018). Identity Theft and Social Media. *IJCSNS International Journal of Computer Science and Network Security*, *18*(1), 43. Retrieved from http://paper.ijcsns.org/07_book/201801/20180106.pdf

Jaihankar, K. (2008). Space Transition Theory. *Crimes of the Internet*, *January 2008*, 283–301. Retrieved from http://www.sascv.org/drjaishankar/theory.html

Jaishankar, K. (2020). Cyber Victimology: A New Sub-Discipline of the Twenty-First Century Victimology. In *In An International Perspective on Contemporary Developments in Victimology* (pp. 3-19). Springer, Cham.

Jaradat, M. A.-K. (2017). Gender Differences in Bullying and Victimization Among Early Adolescents in Jordan. *PEOPLE: International Journal of Social Sciences*, *3*(3), 440–451. https://doi.org/10.20319/pijss.2017.33.440451

Jeesmitha, P. S., & Com, M. (2019). The Impact of Social Media. *International Journal of Scientific Research and Engineering Development*, *2*(1), 229–235. Retrieved from www.ijsred.com

Jisha, K., & Jebakumar. (2014). Whatsapp: A Trend Setter in Mobile Communication among Chennai Youth. *IOSR Journal Of Humanities And Social Science (IOSR-JHSS), 19*(9), 01-06.

Kalule, M. P. (2018). The Legal Challenges of Social Media. *SCRIPT-Ed*, *15*(1), 141–148. https://doi.org/10.2966/scrip.150118.141

Kaplowitz, M. D., Hadlock, T. D., & Levine, R. (2004). A comparison of web and mail survey response rates. *Public Opinion Quarterly, 68*(1), 94–101.

Karim, K. H., & Al-Rawi, A. (2018). *Diaspora and media in Europe: Migration, identity, and integration*. Springer.

Kelfve, S., Kivi, M., Johansson, B., & Lindwall, M. (2020). Going web or staying paper? The use of web-surveys among older people. *BMC Medical Research Methodology, 20*(252). Retrieved from https://bmcmedresmethodol.biomedcentral.com/articles/10.1186/s12874-020-01138-0

Kižina, S. (2015). *Social Media As a New Propaganda*.

KNBS. (2019). *Kenya Population and Housing Census Results.* Nairobi: Kenya National Bureau of Statistics. Retrieved October 16, 2021, from https://www.knbs.or.ke/?p=5621

Kuckartz, U. (2019). Qualitative text analysis: A systematic approach. In *Compendium for early career researchers in mathematics education* (pp. 181–197). Springer, Cham.

Kumar, S., & Somani, V. (2018). *Social Media Security Risks , Cyber Threats And Risks*. *May*.

Kwanya, T., Kogos, A. C., Kibe, L. W., Ogolla, E. O., & Onsare, C. (2021). *Cyber-bullying research in Kenya: a meta-analysis. Global Knowledge, Memory and Communication.*

Lieberman, J. D., Koetzle, D., & Sakiyama, M. (2013). Police departments' use of Facebook: Patterns and policy issues. *Police quarterly, 16*(4), 438-462.

Lindemann, N. (2021, August 9). *What's The Average Survey Response Rate? [2021 Benchmark]*. Retrieved from SurveyAnyplace: https://surveyanyplace.com/blog/average-survey-response-rate/

Luxton, D. D., June, J. D., & Fairall, J. M. (2012). Social media and suicide: A public health perspective. *American Journal of Public Health*, *102*(SUPPL. 2). https://doi.org/10.2105/AJPH.2011.300608

Magufuli, J. J. (2019). *Efficacy of communications regulation in the prevention of content cybercrimes in Tanzania: A case of Dar-es-salaam city.* (Doctoral dissertation, The University of Dodoma).

Makinde, O. A., Olamijuwon, E., Ichegbo, N. K., Onyemelukwe, C., & Ilesanmi, M. G. (2021). The nature of technology-facilitated violence and abuse among young adults in sub-Saharan Africa. *The Emerald International Handbook of Technology Facilitated Violence and Abuse*.

Manyerere, D. J. (2021). Youth Perceptions, Use and Effects of Social Media on Peace and Conflicts in Tanzania. *Ghana Journal of Development Studies*, *18*(2), 48–73.

Modha, S., Mandl, T., Majumder, P., & Patel, D. (2020). Tracking hate in social media: Evaluation, challenges and approaches. *SN Computer Science*, *1*(2), 1-16.

Mohsin Alvi. (2016). A Manual for Selecting Sampling Techniques in Research. University of Karachi, Iqra. University. *Munich Personal RePEC Archive*, *2016*, 1–56.

Muindi, M. (2020). Mitigating the Impact of Media Reporting of Terrorism Case Study of Government Communication during Westgate and DusitD2 Attacks Mitigating the Impact of Media Reporting of Terrorism—Case Study of Government Communication during Westgate and DusitD2 Att. *The International Centre for Counter-Terrorism*.

Munyua, A. W. (2013). *Women and cyber crime in Kenya.* Nairobi: Kenya ICT Action Network (KICTANet).

Naro, W., Syatar, A., Amiruddin, M. M., Haq, I., Abubakar, A., & Risal, C. (2020). Shariah Assessment Toward the Prosecution of Cybercrime in Indonesia. *International Journal,*, 573.

Näsi, M., Oksanen, A., Keipi, T., & Räsänen, P. (2015). Cybercrime victimization among young people: a multi-nation study. *Journal of Scandinavian Studies in Criminology and Crime Prevention*, *16*(2), 203-210.

Nikolaou, D. (2017). Does cyberbullying impact youth suicidal behaviors? *Journal of Health Economics*, *56*(December 2017), 30–46. https://doi.org/10.1016/j.jhealeco.2017.09.009

Nilan, P., Burgess, H., Hobbs, M., Threadgold, S., & Alexander, W. (2015). Youth, Social Media, and Cyberbullying Among Australian Youth: "Sick Friends." *Social Media and Society*, *1*(2). https://doi.org/10.1177/2056305115604848

Nishad, M. (2018). *A Review Paper on Phishing Through E-Mail*. *1*, 1–2.

Ogunlana, S. O. (2019). Halting Boko Haram/Islamic State's West Africa Province Propaganda in Cyberspace with Cybersecurity Technologies. *Journal of Strategic Security*, *12*(1), 72-106.

Oksanen, A., & Keipi, T. (2013). Young people as victims of crime on the internet: A population-based study in Finland. *Vulnerable children and youth studies*, *8*(4), 298-309.

Okuku, A., Renaud, K., & Valeriano, B. (2015). Cybersecurity strategy's role in raising Kenyan awareness of mobile security threats. *Information & Security*, *32*(2), 1.

Olivas, R. N. (2019). *Social sciences Family , Bullying and Cyberbullying*.

Olofinbiyi, S. A. (2021). Exploring Youth Awareness of Cybercrime and Factors Engendering its Proliferation in Nigeria. *African Renaissance*, *18*(4), 319-342.

Omede, A. J., & Alebiosu, E. A. (2020). Social Media and Boko Haram Insurgency in Nigeria. *Fuwukari International Journal of Sociology and Development*, *1*(2), 1-12.

Paat, Y.-F., & Markham, C. (2021). Digital crime, trauma, and abuse: Internet safety and cyber risks for adolescents and emerging adults in the 21st century. *Social Work in Mental Health*, *19*(1), 18–40.

Patel, H., & Prajapati, P. (2018). International Journal of Computer Sciences and Engineering Open Access. *International Journal of Computer Sciences and Engineering*, *6*(10).

Patel, P., Kannoorpatti, K., Shanmugam, B., Azam, S., & Yeo, K. C. (2017). A theoretical review of social media usage by cyber-criminals. *2017 International Conference on Computer Communication and Informatics (ICCCI)* (pp. 1-6). IEEE.

Pawelz, J., & Elvers, P. (2018). The digital hood of urban violence: Exploring functionalities of social media and music among gangs. *Journal of Contemporary Criminal Justice*, *34*(4), 442–459.

PCAK. (2021, April 22). *Recruitment, Vetting and Approval Model*. Retrieved from PCAK: https://pcak.info/recruitment-vetting/

Peters, S. E., & Ojedokun, U. A. (2019). Social Media Utilization for Policing and Crime Prevention in Lagos, Nigeria. *Journal of Social, Behavioral, and Health Sciences*, *13*(1). https://doi.org/10.5590/jsbhs.2019.13.1.10

Petherick, W. (2017). Victim Precipitation: Why we need to Expand Upon the Theory. *Foresic Research & Criminology International Journal*, *5*(2), 2–4. https://doi.org/10.15406/frcij.2017.05.00148

Project, D. C., Waal, A. De, & Gideon, C. (2018). *The Culture of Terrorist Propaganda in Sub-Saharan Africa A Case Study on Al-Shabaab ' s Use of Communication Technologies in Somalia and Kenya*.

Radcliffe, D., & Bruni, P. (2019). *State of social media, Middle East: 2018.*

Radunović, V., & Veinović, M. (2020). Malware command and control over social media: Towards the server-less infrastructure. *SJEE*, *17*(3), 357–375.

Ramirez, F. A., & Denault, V. (2019). *Running head: FACEBOOK IN SEXUAL ASSAULT TRIALS Facebook, female victims, and social media evidence in sexual assault trials*.

Rathore, S., Sharma, P. K., Loia, V., Jeong, Y. S., & Park, J. H. (2017). Social network security: Issues, challenges, threats, and solutions. *Information sciences*, *421*, 43-69.

Richins, S. (2015). Social Media Use in Health. *Emerging Technologies in Healthcare*, *March*, 81–86. https://doi.org/10.1201/b18431-6

Ruangnapakul, N., Salam, Y. D., & Shawkat, A. R. (2019). A systematic analysis of cyber bullying in Southeast Asia countries. *International Journal of Innovative Technology and Exploring Engineering*, *8*(8), 104–111.

Ruggiero, V. (2019). Yemen: civil war or transnational crime? *Critical Criminology*, *27*(3), 503-514.

Security, H., & Integration, R. (2020). *The influence of human security challenges on the effectiveness of regionalism: The Case of ASEAN + 3*. *June*, 0–62. https://doi.org/10.13140/RG.2.2.11916.13446

Seelinger, K. T. (2020). Securing Improved Cooperation. In *In The International Criminal Court: Contemporary Challenges and Reform Proposals* (pp. 37-46). Brill Nijhoff.

Shaari, A. H., Kamaluddin, M. R., Paiz Fauzi, W. F., & Mohd, M. (2019). Online-dating romance scam in Malaysia: An analysis of online conversations between scammers and victims. *GEMA Online Journal of Language Studies*, *19*(1), 97–115. https://doi.org/10.17576/gema-2019-1901-06

Shava, H., & Chinyamurindi, W. T. (2018). Determinants of social media usage among a sample of rural South African youth. *SA Journal of Information Management*, *20*(1), 1–8. https://doi.org/10.4102/sajim.v20i1.827

Silva, C. (2017). Research Design—The New Perspective of Research Methodology. *British Journal of Education, Society & Behavioural Science*, *19*(2), 1–12. https://doi.org/10.9734/bjesbs/2017/30274

SIMElab Africa. (2019). *The Kenyan Social Media Landscape: Trends and Emerging Narratives, 2020.* Nairobi: USIU.

Soomro, T. R., & Hussain, M. (2019). Social Media-Related Cybercrimes and Techniques for Their Prevention. *Applied Computer Systems, 24*(1), 9–17. https://doi.org/10.2478/acss-2019-0002

Stone, R. (2020). *Brandman Digital Repository The Effects of Cyberbullying as it Relates to Social Media: A California High School Assistant Principal and High School Counselor Perspective*.

Stone, R. (2020). Brandman Digital Repository The Effects of Cyberbullying as it Relates to Social Media : A California High School Assistant Principal and High School Counselor Perspective.

Sunday, F. (2021, November 24). *Alarm as hackers now set their sights on start-ups*. Retrieved from The Standard: https://www.standardmedia.co.ke/business/enterprise/article/2001430029/alarm-as-hackers-now-set-their-sights-on-start-ups

Tamori, A., Bhujade, R. K., Sinhal, A., & Professor, A. (2018). Analysis on Whatsapp Security. *International Journal of Ethics in Engineering & Management Education Website: Www.Ijeee.In*, *5*(6), 2348–4748.

Tanvir, S., Matiur, M., & Hossain, F. (2021). Role of Social Media in Spreading Violent Extremism in Bangladesh. *Available at SSRN 3908734*.

Throuvala, M. A., Griffiths, M. D., Rennoldson, M., & Kuss, D. J. (2021). Perceived challenges and online harms from social media use on a severity continuum: a qualitative psychological stakeholder perspective. *International journal of environmental research and public health*, *18*(6), 3227.

Tikhonov, A., & Konovalova, V. (2020). The impact of social media on recruitment: Opportunities, benefits, and challenges. *Smart Innovation, Systems and Technologies*, *172*(2), 415–423. https://doi.org/10.1007/978-981-15-2244-4_39

Tufekci, Z. (2018). How social media took us from Tahrir Square to Donald Trump. *MIT Technology Review*, 18.

Udenze, S. (2017). Is whatsapp messaging subsuming conventional SMS. *International Journal of Advanced Research and Publications, 2*(3), 20-25.

Uhls, Y. T., Ellison, N. B., & Subrahmanyam, K. (2017). Benefits and costs of social media in adolescence. *Pediatrics, 140*(Supplement 2), S67-S70.

Uldam, J. (2018). Social media visibility: challenges to activism. *Media, Culture & Society*, 41-58.

USIU Africa. (2020). *The Kenyan Social Media Landscape: Trends and Emerging Narratives, 2020*. USIU. https://www.usiu.ac.ke/assets/image/Kenya_Social_Media_Lanscape_Report_2020.pdf

van Schaik, P., Jansen, J., Onibokun, J., Camp, J., & Kusev, P. (2018). Security and privacy in online social networking: Risk perceptions and precautionary behaviour. *Computers in Human Behavior*, *78*, 283–297. https://doi.org/10.1016/j.chb.2017.10.007

Vidija, P. (2021, February 18). *Kenya at high risk as cyberattacks continue to plague businesses*. Retrieved from The Star: https://www.the-star.co.ke/news/big-read/2021-02-18-kenya-at-high-risk-as-cyberattacks-continue-to-plague-businesses/

Waechter, N. (2021). Gendered social media cultures between individuality and collectivity. In *Forms of Collective Engagement in Youth Transitions* (pp. 185-206). Brill.

Wahl, O. F. (2003). Depictions of mental illnesses in children's media. *Journal of Mental Health*, *12*(3), 249–258. https://doi.org/10.1080/0963823031000118230

Wakoli, C. O. (2018). Relationship between Exposure to Mass Media and Drug Abuse among Adolescent Students in Secondary Schools in Kenya. *International Journal of Scientific and Research Publications (IJSRP)*, *8*(12), 840–849. https://doi.org/10.29322/ijsrp.8.12.2018.p84104

Walsh, J. P. (2020). Social media and border security: Twitter use by migration policing agencies. *Policing and Society*, *30*(10), 1138–1156.

Walsh, J. P., & O'Connor, C. (2019). Social media and policing: A review of recent research. *Sociology Compass*, *13*(1). https://doi.org/10.1111/soc4.12648

Wambua, I. M. (2020). *Impact of social media on national security in Africa: Case study of Kenya.* Nairobi: (Masters thesis, University of Nairobi).

Wang, Y., & Mark, G. (2018). The context of college students' facebook use and academic performance: An empirical study. *Conference on Human Factors in Computing Systems - Proceedings*, *2018-April*(April). https://doi.org/10.1145/3173574.3173992

Wanjiku, E. (2021). Revenge pornography on the internet: The case of social media in Kenya. *Communicare: Journal for Communication Sciences in Southern Africa*, *40*(1), 151-170.

Whitty, M. T., & Buchanan, T. (2016). The online dating romance scam: The psychological impact on victims – both financial and non-financial. *Criminology and Criminal Justice*, *16*(2), 176–194. https://doi.org/10.1177/1748895815603773

Zappavigna, M. (2016). Social media photography: Construing subjectivity in Instagram images. *Visual Communication*, *15*(3), 271–292. https://doi.org/10.1177/1470357216643220

Zhang, Z., & Gupta, B. B. (2018). Social media security and trustworthiness: Overview and new direction. *Future Generation Computer Systems*, *86*, 914–925.

APPENDICES

Appendix I: Consent Form

Am Sally Soita, student at Kenyatta University undertaking Masters in Security and Police studies, from the department of Security and correctional Science undertaking a research on '**SOCIAL MEDIA INFLUENCE ON PERSONAL SECURITY AMONG THE YOUTHS IN NAIROB COUNTY**.''

The study is beneficial for academic knowledge, policing agencies and personal security on social media.

As a respondent, you are required to participate voluntarily in this study, questions that are not relevant may not need your response, information received will be for academic purposes and strictly confidential.

Contact Information

Student: Sally Soita: 0724645540

Supervisor Dr Njoroge: njoroge.harrison@ku.ac.ke

Participant's statement

have read and understood the contents of this form and therefore accept to take part in the study.

Respondent's signature: Date

Appendix II: Study Questionnaire

Dear respondent,

My name is Sally Soita, Masters Student in Security Management and Police studies at Kenyatta University, undertaking research on "Social Media Influence on Personal Security among the youth in Nairobi City County". I urge you to fill the questionnaire with honesty and confidentiality, the responses received will only be used for academic needs.

Instructions

Please tick where appropriate

Please provide brief answers to the statements given below

SECTION A: Background Information

1. Age

19-25 ( ) 26-30 ( ) 31-35 ( )

2. Gender

Male ( ) Female ( )

3. Occupation

Employed ( )

Job seeker ( )

Student ( )

4. Education level

No formal education ( )

Primary level ( )

Secondary ( )

University ( )

SECTION B: Forms of Social media

5. What form of social media do you frequently use?

Facebook ( )

Whatsapp ( )

Twitter ( )

Emails ( )

YouTube ( )

LinkedIn ( )

Instagram ( )

6. What form of social media is more insecure?

Facebook ( )

Whatsapp ( )

Twitter ( )

Emails ( )

YouTube ( )

LinkedIn ( )

Instagram ( )

7. What crimes have you experienced on social media?

Cyber bullying ( )

Online romance scams ( )

Cyber stalking ( )

Fake jobs ( )

Identity theft ( )

Hacking ( )

8. Have you been a victim of social media crimes?

Yes ( ) No ( )

9. Which form of device do you use to access internet services?

Computers ( )

Laptops ( )

Android phones ( )

Ipad ( )

10. What solutions do you recommend for social media crimes?

……

11. Do you feel safe after joining social media?

Yes ( ) No ( )

12. Do you feel safe after deactivating social media account?

Yes ( ) No ( )

Appendix III: Law Enforcement Letter

SECTION 1

INTRODUCTION LETTER
KENYATTA UNIVERSITY,
DEPARTMENT OF SECURITY AND CORRECTION SCIENCE,
P.O BOX 43844-00100,
NAIROBI, KENYA

Dear Sir/Madam,

Re: Request for Data Collection

My name is Sally Soita, a student of Kenyatta University pursuing a Master of Security Management and Police Studies. As a mandatory requirement of my degree, am conducting a research on "Social Media Influence on Personal Security among the youth in Nairobi City County."

Kindly assist me with necessary information related to this topic, your cooperation will be appreciated, feel free to respond willingly.

Yours faithfully,

Sally Soita

SECTION 2: Personal Background

Am Sally Soita

Born in Bungoma County

Currently a Master's student at Kenyatta University

Am most obliged to receive any questions through the interview

Appendix IV: Questions for Law Enforcement Officers in PCAK

- What are the common social media crimes reported?
- What is the average age of social media victims?
- What are the existing laws in curbing social media crimes?
- What is the penalty for social media offences?
- Do you agree that spending more time on social media predisposes one to be a victim?
- Are most victims females or males?
- What are the challenges encountered in investigation and prosecution of social media crimes?

Appendix V: Work Plan

ACTIVITY	FEBRUARY-NOVEMBER 2018	DECEMBER-JANUARY 2019	1FEBRUARY2019	FEBRUARY-MARCH 2019	APRIL 2019	MAY 2019	JUNE 2019	OCTOBER 2020	MARCH 2021	APRIL 2021	OCTOBER 2021
LITERATURE REVIEW											
CONCEPT WRITING											
CONCEPT DEFENCE											
PROPOSAL WRITING											
PROPOSAL DEFENSE											
PROPOSAL CORRECTION											
DATA COLLECTION											
DATA ANALYSIS											
PROJECT CORRECTION											
SUBMISSION TO GRADUATE SCHOOL											

Appendix VI: Budget

ITEM	UNIT COST IN KSH	TOTAL IN KSH
A)Concept paper preparation		
Type setting	27 pages*20	1080
Printing	27pages*10	270
Copies to department	270*3	813
Sub total		2163
B)Proposal preparation		
Draft copies for Supervisors	6 copies *40 pages*3	720
Departmental defense	10copies*40pages*3	130
Travelling	12months*2000	24000
Internet	12months*2000	24000
Sub total		48850
C)Pilot study		
Printing	3pages *10	30
Photocopy	3*16*3	144
Travelling & other allowances	2000*2	4000
Sub total		4174

D)Data collection

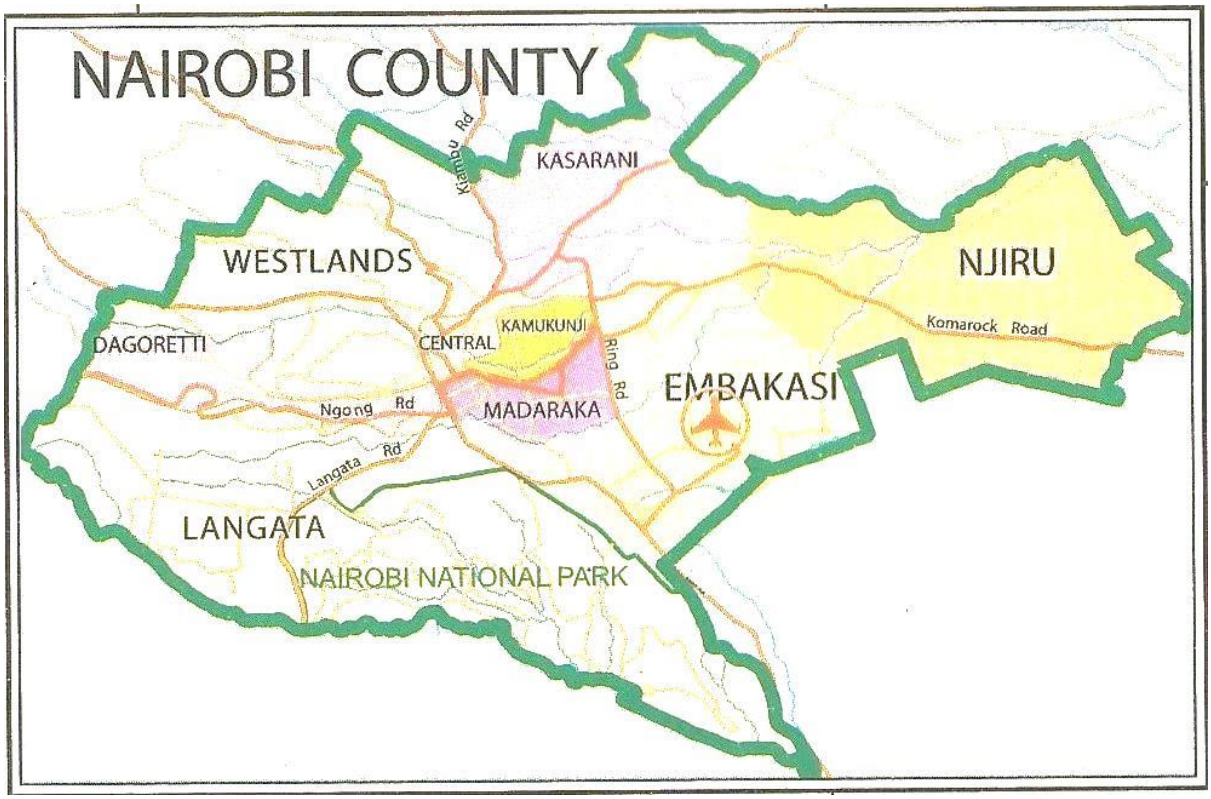
Typesetting and printing	5pages*40	200
Photocopying	5*156*2	1560
Travelling & other allowances	30days*500	15000
Sub total		16760

E)Project preparation

Typesetting and printing	70 pages *40	2800
Photocopying and printing	70 pages *10copies *4	2800
Binding	12copies*50	600
Subtotal		9000

Subtotal	80,947
10% Contigency	8,094.7
GRAND TOTAL	**89,041.70**

Appendix VII: Nairobi County Map



Appendix VIII: Research Authorization Letter

KENYATTA UNIVERSITY
GRADUATE SCHOOL

E-mail: dean-graduate@ku.ac.ke
Website: www.ku.ac.ke

P.O. Box 43844, 00100
NAIROBI, KENYA
Tel. 8710901 Ext. 57530

Our Ref: C159/CTY/PT/38456/2016 **DATE: 8th September, 2021**

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

Dear Sir/Madam,

RE: RESEARCH AUTHORIZATION FOR SOITA NAFULA SALLY – REG. C159/CTY/PT/38456/2016.

I write to introduce **Soita Nafula Sally** who is a Postgraduate Student of this University. The student is registered for M.A degree programme in the **Department of Security and Correction Science.**

Soita intends to conduct research for a M.A Project Proposal entitled, **"Social Media Influence on Personal Security among the Youth in Nairobi City County, Kenya".**

Any assistance given will be highly appreciated.

KENYATTA UNIVERSITY
OFFICE OF DEAN
09 SEP 2021
P.O. BOX 43844-00100 NAIROBI

Yours faithfully,

PROF. ELISHIBA KIMANI
DEAN, GRADUATE SCHOOL

HI/bm

Appendix IX: Approval of Research Proposal From Graduate School

KENYATTA UNIVERSITY
GRADUATE SCHOOL

E-mail: dean-graduate@ku.ac.ke
Website: www.ku.ac.ke

P.O. Box 43844, 00100
NAIROBI, KENYA
Tel. 810901 Ext. 4150

Internal Memo

FROM: Dean, Graduate School

DATE: 8th September, 2021

TO: **Soita Nafula Sally**
C/o Security & Correction Science Dept.

REF: C159/CTY/PT/38456/2016

SUBJECT: APPROVAL OF RESEARCH PROPOSAL

We acknowledge receipt of your revised Research Proposal as per our recommendations raised by the Graduate School Board of 25th August, 2021 entitled **"Social Media Influence on Personal Security among the Youth in Nairobi City County, Kenya".**

You may now proceed with your Data Collection, Subject to Clearance with Director General, National Commission for Science, Technology and Innovation.

As you embark on your data collection, please note that you will be required to submit to Graduate School completed Supervision Tracking and progress report forms per semester. The forms are available at the University's Website under Graduate School webpage downloads.

Thank you.

KENYATTA UNIVERSITY
09 SEP 2021
P.O. BOX 43844 - 00100 NAIROBI

HARRIET ISABOKE
FOR: DEAN, GRADUATE SCHOOL

C.c. Chairman, Department of Security and Correction Science

Supervisors:

1. Dr. Harrison Njoroge
C/o Department of Security and Correction Science
Kenyatta University

HI/bm

Appendix X: Research Permit

REPUBLIC OF KENYA

NATIONAL COMMISSION FOR SCIENCE, TECHNOLOGY & INNOVATION

Ref No: 828628

Date of Issue: 23/September/2021

RESEARCH LICENSE

This is to Certify that Miss: SALLY NAFULA SOITA of Kenyatta University, has been licensed to conduct research in Nairobi on the topic: "Social Media Influence on Personal Security among the Youth in Nairobi City County,Kenya" for the period ending : 23/September/2022.

License No: NACOSTI/P/21/13038

828628

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.