WOMEN'S EXPERIENCES WITH CYBER CRIME A CASE OF NAIROBI COUNTY, KENYA.

LORNA AJWANG' OKETCH

A RESEARCH PROJECT SUBMITTED TO THE AFRICAN WOMEN'S STUDIES CENTRE IN PARTIAL FULFILLMENT FOR THE REQUIREMENT OF THE AWARD OF MASTER OF ARTS DEGREE IN WOMEN, LEADERSHIP, AND GOVERNANCE IN AFRICA OF THE UNIVERSITY OF NAIROBI

2020

DECLARATION

I declare that this is my work and to the best of my knowledge, it has not been submitted to any university or institution of higher learning for examination or any other purposes.

Lorna Ajwang' Oketch
M10/24966/2019

Signature Date 01/09/2021

…………………………………..…………………………………

Supervisors

This research project has been submitted for examination with our approval as the university supervisors.

Dr. Marygorety Akinyi

Signature Date
01/09/2021

Dr. Grace Nyamongo
Signature Date:
GNyamongo 8/9/2021

DEDICATION

I dedicate this work to all those who've been affected in one way or another by cybercrimes. I pray that this research findings will influence implementation and enforcement of the Computer misuse and cybercrimes Act, 2018so as to protect all that have access to ICT which will in turn enable them to concentrate on matters development and improvetheir lives. To my family and friends, who are always my source of support and inspiration. Thank you.

ACKNOWLEDGEMENT

I am grateful to God for His sufficient grace and mercy. Thanks to the Impact (Ed) International, formerly Discovery Learning Alliance (DLA) management and staff. Madam Salome Aloo, the Ag. Country Project Director, Madam Benta Otsyeno, the Training and Outreach Manager, allows me to research. Dr. Marygorety Akinyi and Dr. Grace Nyamongo, my supervisors and lecturers at the University of Nairobi, thank you so much for your insight as you read and reviewed my reportable to correct my work from the very beginning. I wish to thank all those who made this possible and to those whom I haven't mentioned here and were with me every step of the way, thank you and stay blessed.

TABLE OF CONTENTS

Contents

ABSTRACT.. 1

CHAPTER ONE 2

1.0Background of the study..2

1.1 introduction...2

1.2 Statement of the Problem 3

1.3 Research Objectives...4

1.3.1 General Objective 4

1.3.2 Specific Objectives 4

1.4 Assumptions...5

1.5 Justification of the study..5

1.6 Scope and Limitations of the Study 5

1.7 Definition of Terms...6

CHAPTER TWO 7

2.1.1 Internet and Women 7

2.2 Forms of cybercrimes against women..8

2.2.1 Online Harassment 8

2.2.2 Pornography 8

2.2.3 Women Trafficking...8

2.2.4 Morphing 8

2.2.5 Flaming 8

2.2.6 E-Mail Harassment...9

2.2.7 Internet defamation 9

2.2.8 Cyber stalking..9

2.3 How does cyber crime affect women?..9

2.4 Coping mechanisms to curb or mitigate cybercrimes..10

2.5 Theoretical Framework..11

2.5.1 Relevance of the Theory of study..11

CHAPTER THREE..13

3.1 Introduction..13

3.2 ResearchDesign..13

3.3 StudyPopulation..13

3.4 SamplePopulation..14

3.5 SamplingProcedure..15

3.6 Data CollectionMethods..16

3.6.1 SurveyTechnique..16

3.7 Data processing andanalysis..16

3.9 Ethical considerations..16

CHAPTER FOUR..18

4.1 Introduction..18

Prevalence of Cybercrimes on women..Error! Bookmark not defined.

CHAPTER FIVE..36

5.1 Introduction..36

REFERENCES..45

APPENDIX 1..51

Questionnaire..51

LIST OF TABLES

Table 1Sample Population... 14

Table 2 Sampling of respondents 15

Table 3 Age of Respondents …………………………………………………………………………18

Table 4 Marital Status of Respondents……………………………………………………………….19

Table 5 Reasons for Internet use………………………………………………………………………20

Table 6 Cyberstalking ……………………………………………………………………………….25

Table 7 Perpetrators by gender……………………………………………………………………….26

Table 8 Online proximity…………………………………………………………………………….32

Table 9 List of information posted by woment online……………………………………………….33

LIST OF FIGURES

Figure 1 Widespread prevalence of cybercrimes against women ………………………………………21

Figure 2 Widespread presence of online harrassment against women…………………………………..24

Figure 3 Feelings expressed by victims of cybercrime………………………………………………..29

Figure 4 Measures taken by victims to mitigate cybercrimes……………………………………………30

ABSTRACT

This a cross-sectional descriptive study of the women's experiences of cybercrimes in Nairobi County, Kenya. The study expressly set out to determine the forms of cybercrimes experienced by women, examine the prevalence of cybercrimes against women, and the effects of cybercrime on women. The study findings indicate that respondents enjoy 90% of internet access either at home, office/work, cell phones, modem, and cyber café. Out of the 140 respondents surveyed, 45% (63) were single, 32%(45) were married, 16%(22) were separated/divorced, and 7%(10) reported to be widowed. Women encounter an array of cybercrimes, including online harassment, cyberstalking, received obscenities, threats online, sexual harassment, privacy exposed, impersonated, reputation sabotaged, private photos posted online without their consent/approval, computer disabled. Online harassment and cyberstalking are the most common, at 77.6%(109) and 76.1%(107), respectively. Out of the 140 respondents, 53.2%(74) reported having received sexually harassing advances, messages, or pictures; 42.8%(60) did not consider the passages as harassing. Risk factors associated with increased exposure to cybercrimes included those with many social online accounts, updating their statements frequently, especially with a controversial topic. Most of the time, online users do not set their accounts to privacy settings, adds strangers to their friends' lists, and post personal information. From the findings, the perpetrators of cybercrimes are not necessarily men as 44.2%(62) of the perpetrators were reported to be male, 42.7%(60) were women perpetrators, and 12.9%(18) gender was unknown.

The study concludes that majorityuse the internet for social networking and work/study,making them more susceptible to cybercrime. Online harassment and cyberstalking is an issue that needs to be addressed. At times, online contacts end up in offline communications,leading to actual physical harm that cause emotional and psychological distress. The study recommends that women using online resources should make use of the security settings put in place to limit online exposure, and increase the offender's risk. The government through the law enforcement agencies should impelement and enforce the Computer misuse and cybercrimes Act, 2018 so as to protect internet users against cybercrime.

CHAPTER ONE

1.0 BACKGROUND OF THE STUDY

1.1 Introduction

Internet use continues to positively and negatively influenceevery society's social, economic, cultural, and political aspects. While the internet has provided a safe space for women to enjoy their basic human rights like the power to act, speak or think as one wants, right to knowledge and confidential communication; it has also extended the same benefits to cyber criminals who use Information Communication Technology (ICT) for criminal activities. Cybercrime is an illegal activity undertaken online and is divided into three major categories, a crime against humanity, property and the government/ state (Duggal 2002). This research study will focus oncybercrime against the woman.

Cybercrime includes but not limited to child pornography, online harassment, and cyberstalking. Online harassment and cyber stalking are the focus of this study. The internet being anonymous provides a haven for perpetrators of cybercrimes. Online harassment can either be sexual, racial, or religious in nature which results in the violation of privacy. Cyberstalking is a crime when there is repeated annoying or tormenting pursuit of an individual or individuals using electronic communications even after being asked to stop. Wykes(2007a) states that it is persistently contacting someone even after being asked to stop, making inappropriate sexual advances towards someone, and it can either be through intimidation or blackmail.

Online harassment can either be direct or indirect where direct online harassment includes threats, intimidation, bullying via messages sent directly to the victim’s communication media is divided into two categories direct and indirect harassment where direct harassment includes threats, bullying, or intimidating messages sent directly to the victim communication mediums e.g. mobile phones. Indirect online harassment includes spreading rumors about the victim in various internet discussion forums, subscribing the victim to unwanted online services, posting personal or confidential information about the victim in online dating or sex services, impersonation, or posting of nude pictures of real women with or without their consent (Harvey 2003).

There isgrowth in internet use and other electronic communications, with over 59 million internet users worldwide, there were 22.86 million of them Kenyans (CAK , 2020) which means that the number of internet users in Kenya increased by 3.2 million(+16%) between January 2019 and January 2020. This growth in internet use has brought with it an increase in the ,misuse of ICT. These offenses directly affect individual victims as they fear for their safety and personal well being. (Yah 2006). Simultaneously, security concerns over internet use are usually ignored because there is that belief that such communications are not dangerous since they are not physical hence they tend to be easily overlooked. Usage of cell phones and the online platform to stalk, abuse, traffic, intimidate, and humiliate women is observable in many countries, including Kenya.

Most women who have access to the internet in Kenya are not aware of the internet's dangers. There is also a lack of awareness of the Computer Misuse and Cybercrimes Act, 2018; which makes it even more difficult to punish perpetrators of cybercrime. It has become necessary to estimate the prevalence of cybercrime among women, forms of cybercrime affecting women, the online activities that are putting them at more risk of being cybercrime victims, document how women are affected and how they are reacting to cybercrimes. (Kenya Gazette Supplement No.60 (Acts No 5).

This research attempted to create awareness of cybercrime on women by estimating the prevalence of cybercrime against women, looking at the forms of cybercrimes affecting women, documenting online behavior that is a risk factor for being attacked online by cybercriminals. The research also sought to identify measures women employ to use the internet safely, how this affects their empowerment safely and document their knowledge level on safety on the internet. Due to information networks' global nature, there is an ever-growing vulnerability to online harassment and cyberstalking, mainly directed towards women.

1.2Statement of the Problem

Advent of ICT has provided unrivaled chance for women to make use their abilities to improve their quality of life and contribute to society's welfare. Cell phones, and social mediahave become an efficient communication tool. Kenyans have ease of internet access through mobile phones, with 52.06 million mobile subscribers. The number of mobile connections in Kenya in January 2020 was equivalent to 98% of the total population **(**Communications Authority of

Kenya (CAK). The Internet offers new opportunities for working out deals with an all inclusive autonomy, however activists have failed to challenge the misuse of the intenet. (Scott et al. 2001). Women are more susceptible than men as data show that 73% of women and 27% of men are stalked online. Cybercrimeshave in most cases lead to stalking in the real world (Working to Halt Online Abuse (WHOA) (2010),

There is a need to document the prevalence of cybercrimesagainst women, forms of cybercrimes mainly affecting women, determine how these cybercrimes are affecting women, and explore the online activities that put women at risk of online attacks with a view of creating awareness amongst women on the dangers of the internet and safety precaution when utilizing the internet. This will determine the women's knowledge of safely navigating technology resources without increasing the risk of abuse for safer webspace. It will be a milestone to enable women to communicate without restraintto contributein all the spheres of development within the society.

The assumption is that ICT has contributed greatly to addressing gender imbalances however it has also reinforced the existing structures of gender inequlities. The internet has blurred the line between private and public by allowing cyber criminals to access and misuse personal information to target women which as a result continue to reinforce inequlities. Women contribute to development by utilizing online resources but this is limited due to the fear of online harassment and cyberstalking. Cybercrimes take away women’s safe space onlinetherefore denying them the ability to exploit ICT for their own development.

1.3 Research Objectives

1.3.1 General Objective

To investigate the impact of cybercrimeson women.

1.3.2 Specific Objectives

1 To determine the different forms of cybercrimes experienced by women

2. To examine the prevalence of cybercrimes against women.

3. To explore the effects of cybercrimes on women

The study sought to address the following questions:

1. What are the different forms of cybercrimes experienced by women?

2. What is the prevalence of Cybercrimesagainst women?

3. What are the effects of cybercrimes on women?

1.4 Assumptions

The study was guided by the following assumptions that;

1. Women are victims of Cybercrimes.

2. Cyberstalking and online harassment are the primary forms of crimes women face online.

1.5Justification of the study

Increased internet access is making technology an essential resource for women. However, if not understood and used strategically, technology may increase itsvulnerabilities. This study sought to gain insight into cybercrimes against women in Nairobi county. By documenting these experiences, it will create awareness and influence the implementation of the Computer Misuse and Cybercrime Act 2018 which has clearly set guidelines on how to curb and mitigate cybercrime. Marxist theory can be applied in understanding technology and cybercrimes in that ICT has become part today's society. Marx referred to production as a technical process as it involves technology and great success has been achieved by man interms of technology however, it has also been used to render other human beings powerless hense alienation renders powerlessness. Women are directly hit by cybercrimes, and their access to the use internet hindered.Women have been harassed and stalked online; in some instances, women's communication online is hampered. They are forced to use their meager resources to mitigate cybercrimeon them. Other research studies have mostly focused on the offense against the children, property, and government/state. This project focuses on women.

1.6 Scope and Limitations of the Study

This study was carried out in schools that work under the Impact (Ed) International in Nairobi County. The study targeted 146 participants; however, 140 questionnaires were returned for analysis. The issue under investigation was sensitive. It bordered on single issues that are rarely discussed in public, and this presenteda challenge in terms of data collection and exploration of the problem. It was quite a challenge getting information from respondents who felttoo invasive of their privacy. The sample wasdrawn from the staff working with schools under theImpact (Ed) International in Nairobi,further limited the generalizability to women at large. The study determined itself to Nairobi despite the country's immense growth of the Internet and related technology, which would be quite taxing if it were to be explored.

The other limitation was the growth of ICT in the country, and that not many studies have been done in this respect. Therefore, it wasn't easy to compare available data and have literature reviewed based on local research. There is limited local literature on the subject, and consequently, the study relied mainly on foreign literature. Therefore, the literature review hadsignificant international content. This study focuses on women in Nairobi County and its environs, it relied on the fact that Internet access is 90% to all women, but this may not be the case with other parts of the country that are less developed up.

Further, it's not the case with all the Kenyan women in society. The situation elsewhere is that the internet remains inaccessible to the women, hindering their full participation in the ICT revolution. There is a possibility that most women still don't have access to the Internet.

1.7Definition of Terms

Cybercrime means any activity online that leads to a violation of the privacy of communication, democracy, and freedom of expression. Online harassment and cyberstalking constitute cybercrime.

Online harassment means any behavior where one uses information and Communication Technology(ICT) to annoy, or torment someone emotionally, psychologically, or physically.

Cyberstalking means experiencing any one or many forms of online harassment, which must cause fear of harm to a woman on two or more occasions. Stolen identity qualifies to be stalking without causing concern or being repetitive.

CHAPTER TWO

2.0 LITERATUREREVIEW

2.1 Introduction

Theliterature review sought to bring out present knowledge oncybercrime against women, their experiences with cybercrime and identify gaps that further expose them to cybercrime. By identifying these gaps it will motivate the study to advance the body of knowledge on women's experiences with cybercrime. The aggresive growth of the internet corresponds with the diffusion of deliquent behavior within this environment. To get an indepth insight into cyber crime this review highlights the relationship between internet and women, forms of cybercrimes against women and the strategies women are using to address this vice.

2.1.1 Internet and Women

According to Scott et al.(2001) internet on women's lives provides a useful framework for evaluating internet and women. Cybercrimes can be counterproductive for feminists in that if the internet envrironment is hostile, women might opt to stay away from it consequently hampering attempts to secure equal particiation. Internet has made the world a 'global village' where information can be accessed with the click of a button, however it remains inaccessible to women because of the rise in incidences of cyberstalking and online harassment.

This research will favour internet feminism which grew as a result of digital media and new information and communiation technologies which have been credited with potential of simultaneous empowerment and suppression or disempowerment of humanity. Internet possesses the power to exclude non-users, divide the world into the information-rich and the information-poor which has reinforced different forms of oppression, sexism, racism and homophopia. The danger posed on the internet to women which is a central concern of this research outlines the internet's characteristics including the easy manipulation of identities. Elm and Sunden (2007).

Yar (2006) observes that the internet renders women susceptible to cybercrimes. Cybercrime against women including cyberstalking and online harassment is taking alarming portions with studies showing that about 60% of all the websites have sexual content, 25 % of them solicit their visitors. Nearly 13% of surfers go to these sites voluntaritly while the rest are lured pictorially. The increasing populatity of chatrooms and personal data susceptibility to criminals access makes women and children soft targets for many cybercrimes. In India 45% of Internet crimes target women (Duggal 2002).

2.2 Forms of cybercrimes against women

2.2.1 Online Harassment

The cybercrime on women, and the severe effect of this harassment, requires a reconceptualization of how online harassment is understood. The virtual nature of the internet has allowed criminal activities to occur even with no physical contact between the perpetrator and the victim.

Online harassment includes and is not limited to the below crimes:

2.2.2 Pornography

This is in the category of content-related offenses in that according to Scott et al. (2001), the internet is used as a tool for the production, storage and dissemination of sexually demeaning content and explicit images of women and children. Adam (2002:133) observes that in pornography there is bodily invasions of privacy as bodies are looked at or subjected to surveillance; or bodies being violated and watched online. The complicated nature of online harassment constitutes its uniqueness. Wall (2005:84) indicates that "such activities do not require direct physical expression, the victim nevertheless will feel the violence of the act."

2.2.3 Women Trafficking

Human trafficking is the process through which individuals are placed or mainataned in an exploitative situation for economic gain. Trafficking can occur within a county or may involve movement across borders. Women are trafficked for forced and exploitative labour in factories, farms or private households, sexual exploitation and forced marriage. The Internet has become a place for promoting global trafficking. Sex tours for economic gain are advertised where men exchange information on where to find sex workers and describe how they can be used and even write reports on their escapades. (United Nations Human Rights office of the High Commisioner report on Human Rights and Human Trafficking Fact sheet No. 36)

2.2.4 Morphing

This refers to editing the original picture by an unauthorized user or fake identity and reposting it and/or uploading it on different websites. Morphed photographs place victims's faces on another usually a nude body. This violating information haunts the victim as the information cannot be erased as information on the internet is transitory, difficult to stop, retract or delete.

2.2.5 Flaming

Spender (1995) and Williams (2006) define flaming as a specific form of harassment via text which appears to be sexual coercion meant to to drive the victim away from the centre of power. Williams (2006), examining what he terms 'derisory textual performances,' explores several forms of harassment, predominantly directed towards women online which includes sexual harassment.

2.2.6 E-Mail Harassment

This is using electronic media to blackmail, threaten, or bully individual(s). includes blackmailing, threatening, bullying, and even cheating via electornic mail. Electronic-mail harassments are similar to letter harassment but it creates problemsbecause it can be shared real-time, widely and under a short period of time.

2.2.7 Internet defamation

Internet defamation includes libel (written defamation) and slander(making false spoken statement damaging to a person's reputation). This takes place with the help of computers and the internet.

2.2.8 Cyberstalking

Cyberstalking is online harassment that is repetitive and causes fear of personal safety. It includes sending obscene images, sexually harassing messages, sending threatening pictures, impersonation, reputation sabotage, and obtaining confidential information without permission.

Spitzberg&Hoobler (2002) and (Bocij 2004). Online and offline stalking are characterized by the offenders desire to assert control over the victim. This confirms the significant evidence of gender disparity in both online and offline stalking. Study findings indicate that online and offline stalking shows women's predominance as victims and males predominance as offenders (WHOA, 2010).

According to Ellison (2001) men tend to be more antagonistic in their online interactions and use intimidation tactics to dominate and control online discussions.According to an examination of the personal effects of cyberstalking done by Ashcroft (2001) and Wall (2007:84)findings show that although such online actitivies do not require a direct physical contact or expression, the victim will feel the violence of the act and may bear long-term psychological scars as a consequence.

Adam (2002) consideredcyberstalking as a gendered from of cybercrime and classifies it as an extreme form of online harassment; for it to take place direct physical contact may not be a necessary prerequisite which makes it even more dangerous to women.

2.3 How does cybercrime affect women?

According the UN report (2006) about95% of inappropriate behaviorin online spaces are aimed at women and come from partners or former male partners with ICT tools being used to perpetrate cybercrimes against women. Lee (1998) points out that despite all these reported cases of online harassment and cyberstalking , these cybercrimes seem to be absent from the list of those who advocate for women's rights. According to Wall (2007), the ease of access to personal information online facilitates incidences of online harassment. While people are affected by cyberstalking a survey done by WHOA (2010) on the characteristics of 'victims' found that amongst users from the ages of 18-32, victims are predominantly female .

The UN Secretary-General report in 2006 recognized cybercrime as the new forms of violence against women developed with the advent of ICT. In this report member states were urged to acknowledge crimes committed online are on the rise though most of the statistics is sketchy and most of the existing laws and policies on ICT have not been effectively implemented. Cybercrime can take various forms including threatening or sexual messages delivered via electronic media. Victims find these communications a nuisance, emotionally draining, and fear as some of the consequences. These messages may escalate to severe forms of harassment including cyberstalking (Bocij, 2004). With the increase of internet usage online harassment and cyberstalking cases are on the rise among the young people (Finn, 2004). Concepts about offline harassment is equally regarded as applicable to explaining online harassment where cybercrimes also have emotional burden on victims which leads them to fear for their lives or distress, much like real-world stalking and harassment (Bocij , 2004).

2.4Coping mechanisms to curb or mitigate cybercrimes.

Internet service providers offer protective and privacy security tools that filter or block communications from specific individuals who misuse the internet. One way of addressing cybercrime is education and empowerment. There is a need to empower women to exploit ICT resources while protecting themselves from criminals effectively. There is also need for raising awareness and capacity building on information security amongst the priority strategies of addressing cybercrimes from a social perspective. Women who are being continually harassed change their addresses hense losing essential contacts. Cybercrimes due to their virtual nature are easier to commit, difficult to detect and often hard to locate due to the internet's geographical indeterminancy. Many women with the excitement of the Internet have their eyes too blurred to notice the dangers lurking. (Brenner 2000).

There should be a strategy devised not to protect women from online harassment and cyberstalking but to empower them to defend themselves. Cybercrime is avoidable, and greater awareness and education on internet safety are necessary to provide Internet users and especially women, with the knowledge and tools to prevent harassment. According to research done by WHOA(2010), the five most common communication means were facebook, wattsapp, emails instant messaging, message boards, websites, and chat as ICT evolves.

2.5 Theoretical Framework

The Marxism Theory

Marxism theory can used as a tool to understand contemporary society through the concept of production and technology in that technology having become part and parcel of the present community. Marx states that production is a technical process that involves technology hence man has made a lot of effort to gain control over nature using technology. He has gained great success by obtaining large degrees of control over nature, time and distance. According to Marx alienation renders man powerless in that as much as he has achieved great success in technology he has also managed to separate himself from the people around him. Despite all the achieved successes in technology man has become an object or material in the contemporary technology leading to powerlessness an aspect of new technological culture which has deprived him of physical interactions/relations. Cybercrimes such as bullying, defamation, cyberstalking online harassment occur in a virtual environment but it affects people in their day to day lives. It is not easy deal with these online crimes in the physical because internet users are not aware of the dangers that lurk on the internet and the existing laws that protect them.

2.5.1 Relevance of the Theory ofstudy

The elements of Marxist theory hold for cybercrime as those who spend most of their time online networks may also develop emotional connections withothers despite the physical distance separating them (Bocij 2004). The online networking sites allow individuals to share confidential information and pictures/photos exposing them to cyber criminals or making them potential targets to would be harassers. The anonymity provided by the virtual environments increase the likelihood of individualsharassing their victimsonline without fear of being caught (Patchin and Hinduja 2007).

Herring (1999) highlights that online connections are patriarchal in nature which further complicates the process of communicating; interactions between users may take an aggressive adversarial tone where individuals attempt to dominate one another through linguistic conflict.

For instance female users who are interested in technology have reported a high degree of sexual harassment or hostility from others online thus gender affects who would be a likely target for online harassment. Lack of basic ICT skills have also played a role in exposing someone to cybercrimes compared to a skilled user who is better prepared to deal with threats online. The role of guardianship is to help internet users navigate technology resources safely by using computer programs for example antivitus programs, firewall, regularly updating protective software. This underlines the need for awareness and education for women. Results findings on a research study conducted on the computer hacker subculture found that womenof their computer-related baviour or precautions but because of their gender.   (Taylor et al. 2006).

CHAPTER THREE

3.0 METHODOLOGY

3.1 Introduction

Thischapterpresentstheresearchdesign,targetpopulation,sample design and sampling methods, data sources, data collection instruments, and the data analysis and presentation techniques employed to conduct thisresearch.

3.2 ResearchDesign

Thestudyemployed across-sectionalmixed methoddesignwherebothqualitativeandquantitative datawerecollectedandanalyzed.Questionnaireswereadministeredtotherespondents. ThepurposewastogetinformationonCybercrime.146questionnaireswereadministered proportionally per school in the mentioned counties guided by the teachers' ratios. Out of the 146 questionnaires, 140 were returned. Purposivesamplingwas used asanindicationoftheexistingcybercrimes to sought the life stories identified. Participantresponseswereanalyzedtoexploreevidenceonwomenbeingvictimsofcybercrimes,theformsofcybercrimetheyexperience,andhowtheyareaffected.Animportant aspectthatthisstudysought to determinewaswhether,during a victim's harassment,one feared for theirsafety.

3.3 StudyPopulation

This refers to the population of the subject under study. This research focused on female teachers under the schools covered by Impact Ed International in Nairobi County. The total number of femaleteachersinthese schools is 2191.Thetablebelowshowsthenumberof femaleteachers per sub-county who constituted the study population. The information was collected from the school registrars in the respectiveschools with the support of Impact Ed International.

Table 1Sampling of Teachers

Sub-counties	**Female Teachers**
Njiru and Embakasi	1118
Mathari and Starehe	226
Makadara and Kamukunji	125
Westlands and Kasarani	350
Dagoretti, Kibra and Langata	372
Total	**2191**

The information above was collected from the school registrars in the respectiveschools with the support of Impact Ed International.

The teachers' age varies from 18 – 60 years. All teachers have access to the Internet, and they are trained in necessaryICTskills.Alltheteachershavetheminimumskillstoenablethemto accessthe internetand utilize internetresources.

3.4 SamplePopulation

The formula used to calculate the sample sizes:

n =N/ {1 + N (e2)}

Where:

n: Sample Size N: Population

e: Precision Level - 92% (Cochran, 1963; and Israel, 1992).

Usingthe formula n =N/ {1+N (e2)}

Sample Size = 2191/ {1+2191 (0.08)2}

Sample Size = 146

Table 2 **Sampling of Respondents**

Sub-counties in Nairobi	**Female teachers**	**Sample Size**
Njiru and Embakasi	1118	75
Mathari and Starehe	226	15
Makadara and Kamukunji	125	8
Westlands and Kasarani	350	23
Dagoretti, Kibra and Langata	372	25
Total	**2191**	**146**

Table 2 shows that with a population of 2191 from all the eleven sub-counties, the sample size was established to be 146 taking a precision level of 92%. Israel (1992) shows that samples obtainedfromaprecisionlevelof±10%providean adequaterepresentationofthepopulation.

3.5 SamplingProcedure

The probabilisticstratifiedrandomsamplingstrategywasadopted.EachSchoolwastakentobea stratum. The number of questionnaires administered per school depended on the number of female teachers per school. The female teachers' ratiowas used to determine the number of questionnaires administered perschool.

Seventy-five questionnaires were administered to Njiru and Embakasi schools, 15 to Mathari and Starehe schools, 8 to Makadara and Kamukunji schools, 23 to Westlands, and Kasarani schools, and 25to Dagoretti, Kibra, and Langata schools.Thefemaleteachersadministeredwiththequestionnairesineach schoolwerethe ones that answered yes to the question "have youbeenharassedonline?"and wereaskediftheywere willingtosharetheirexperience.Thosewho agreed were requested to write a narrative on their experience, what exactly happened, their feelings,andtheimpacttheharassmenthadonthem.Thedescriptiongivenbyrespondents who have experienced online harassment or stalking and was willing to provide a narrativeoftheincidentwasrecordedasalifestoryandanalyzedinthisstudy.

3.6 Data CollectionMethods

3.6.1 SurveyTechnique

The study adoptedsurvey research method for data collection. The interviewer-administered questionnaires to all the 146 teachers, filled and checked for completeness. The complete questionnaires were 140.

The questions were designed to elicit answers pertinent to the prevalence, forms, and effects of cybercrimes on women. The questionnaires contained questions on demographics, internetaccess,onlinebehavior,onlinesocialnetworks,informationprovisiononline,online harassment, and stalking. The questionnaireswere pretested before beingadministered.Pretesting involved administering the questionnaires to 10 respondents selected randomly from a group of school administrators who were not included in the final sample. Adjustments on the questionnaire was made after the pre-test based on the feedback.

3.7 Data processing andanalysis

The research purpose and the research questions guided the process of analyzing the data. The data used in the study was collected by use of questionaires. The researcher administered 146 questionairres and out of those 140 were returned which accounted for 95% of the total number of questionairres administered.

3.8 Summary of the data collection methods

Qualitative data obtained through life stories and from open-ended questions on the questionnaire were analyzed manually. This is presented in the form of verbatim quotes and explainedinlightofthe literaturereviewed.Quantitativedatawere analyzedusingthestatistical packageofthe socialscientist(SPSS).Theresultsofthedataanalysisarepresentedinfrequency tables andfigures.

3.9 Ethical considerations

Approval to carry out the research was obtained from The University of Nairobi; African

Women’s Studies Cente (AWSC) as well as Impact (Ed) International administration. Informed consent from the respondents on information was sorted whereby the respondents were made to understand the purpose of the study and were to either agree or disagree. Strict confidentiality and anonymity was observed. Respondents were assigned serial numbers for the data collection tool and the number did not have any link with repondent’s name or the school that she came from. Confidentiually was also ensured during data collection through use of pseudonames in cases where verbatim quotes were obtained.

The study having been conducted during the COVID-19 period the researcher ensured that all the Ministry of Health guidelines were followed so as to protect both the respondents, researcher and all involved in the research process.

CHAPTER FOUR

4.0 DATA ANALYSIS ANDPRESENTATION

4.1 Introduction

Findings on the women’s experiences with cybercrime are presented on this chapter. It also explores online activities that increase the risk of cybercrimes on women. The findings are presented based on the survey questions which were dealt with considering different questionnaire items and life stories narratives.

4.2 Socio-Demographic Characteristics of Respondents

Demographic characteristics such as age and relationship status are considered in current estimates of cybercrimes' prevalence on sample population. The sample consisted of 140 women.

4.2.1 Age of Respondents

This study was interested in knowing the respondents' ages to determine the commonness of onlineharassmentandcyberstalkingbyageacrosscybercrime forms.Dataobtained from the field regarding the ages of the women were analyzed and presented.Respondents aged between 18-30 years were 25.5% (37), 62.5%(86)aged31-40and12%(17)aged 41andover.Themeanageofthesamplewas32years.Respondentsunder40experienced 88% online harassment, while those over 40 experienced12% as presented in the table below.

Table 3

Age	**Respondents**	**%age**
18-30 years	37	25.5%
31-40 years	86	62.5%
>41 years	17	12%
Total	**140**	**100%**

4.2.2 Marital Status of the respondents

This was deemed necessary for this study to find any correlation between marital status and Cybercrimes. Relationship status is presented as single, married (including living with someone), divorced, separated, and widowed.

The study found out that 45%(63)oftherespondentswerenot married,32%(45)married,while those separated/divorcedwere 16%(22)and widowed7%(10).The study found out that the majority (68%) of the respondents were not living with spouses. However,23 of the marriedwomendeclaredthattheyhadfirstinteractedwiththeirboyfriends online, who later became their husbands.

Table 4: Marital status of the respondents

Marital status	Respondents	%age
Single	63	45%
Married	45	32%
Separated/divorced	22	16%
Widowed	10	7%
Total	**140**	**100%**

Therefore, the study sought to establish internet access and usage by respondents, as explained in the following sub-section.

4.2.3 Internet Access andUsage

Datawassoughttodeterminetheavailabilityofthe internet.Alltherespondentsreportedhaving access to the internet at the following places; Work/Office,Home,Public Wireless, Cyber Café, Cell Phone, modem. To determine what women did most on the Internet, data on reasons for internet use was collectedandshown inTable4.2.3 below.

Table 5: Reason for internet use

What do you use the Internet for?	**Number of respondents using Internet Service**	**Percentage**
Chat rooms	13	9.2%
Email	32	22.8%
Social Networking sites (such as Facebook)	41	29.4%
Instant messaging	9	6.6%
Study/Work	41	29.4%
Other	4	2.7%
Total	140	100%

The majorityoftherespondentsreportedusingthe internet forsocialcommunication, study, and work, which accounted for 58.8% of the total internet usage.The rest used the internet for emails (22.8%), chats (9.2%), instant messaging (6.6%).

The researcher further sought to establish widespread cybercrimes on women, as demonstrated in the subsection below.

4.3 The widespread presence of cybercrimes againstwomen

Cybercrimes' overall lifetime presence on the sample members was measured as the percentagebywhichthewomenreportedtohavefallenvictimtoonlineharassment and Cyberstalking.

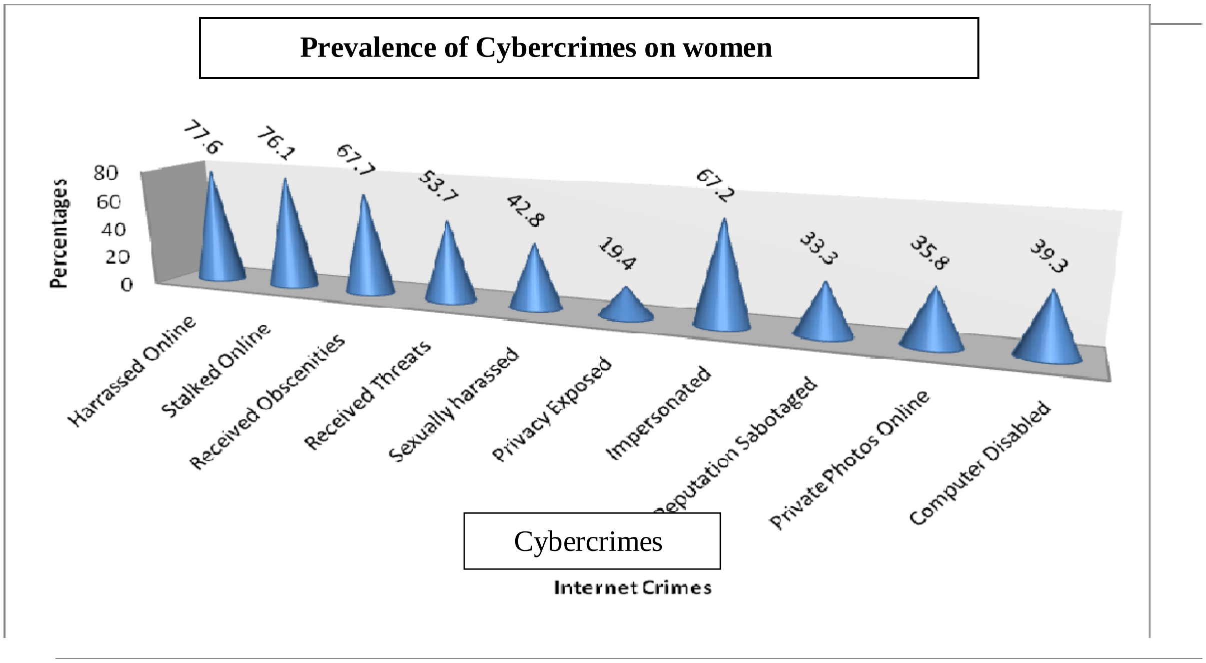


Figure 1Widespread prevalence of cybercrimes against women

Cybercrimeswerecommon amongwomen,withonlineharassment being 77.6% (109) prevalent and Internet stalking being 76.1% (107) dominant. The respondentswereaskedhowtheywereharassedonline. The majorityreportedthattheywere victimsofonlineharassmentandCyberstalkingleadingtoannoyancethattormentedthem emotionally,psychologically,orphysically.Thisisevidencedbyonerespondent'saccountof her online experience andfeeling:

> "*My boyfriend took nude photos of me. When we broke up, he kept threatening me that he would post the images online, but I thought it was a joke and did not know it would haveany severe effects on me. He posted nine nude photos of me, which clearly showed my face on Facebookandtaggedallmyfriends.Ithinkmyfriendsorderedotherpeople,andwithinaday, my photos had been seen by so many people. I later locked myself in my house and felt like committing suicide. I did not leave my room for one and a half weeks. One of my close friends visited me one day andtoldmeshehadseenmynudephotosonseveralwebsites.Allthesephotoshada caption of my name. She counseled me; I explained to her what happened. She understood that she took me through all the websites she had seen the photos. I was in shock at how the images had spread like bush fire. I did not want my parents to learn from*

> *strangers,andIhadtoactfastandtellthem.Itwasverydifficultapproachingandexplaining the embarrassing events tothem.*
>
> *I even thought of changing my names. Because in whatever new community I join, I sometimes notice knowing glances of what they may have seen. Three years later, I am now recovering and have done my best to change my outlook, but this will forever haunt me. I have tried to write to the website managers of the sites my pictures feature to encourage them to delete, but it seems like it is part of their business, as it's only two of the fifty-three websites that am aware of have honored my delete request.*
>
> *If I knew I wouldhaveagreedtoeverything,myex-boyfriendwantedtoalleviate such a situation. But it is too late. I now don't engage in any activity that may give me publicity because eventually, it ends up being negativepublicity.*
>
> *I know I was a nicknamed porn star, and I pray to God that these things don't one day get abovemetocommitsuicide,assometimesIfeelit'stheonlysuresolution.IfIcannot take those photos away, then I can go out. Everything sometimes seems to be so meaningless,especiallywhenIhavetofacemyparents.Ihavegoneto counseling,butitdoesnot help much. I don't browse the Internet anymore, and I have developed a technology phobia. I will also never relate to a man. Sometimes I wonder there is nothing that can be done to my ex for having spoilt my life. Where can I turn to avenge him for what he caused me and fortheextremeinfringementofprivacy?"(36yearsold)*

The above evidence shows the feelings of a woman who has experienced cybercrime. Accordingly, this demonstrates how the crime is committed with impunity. This makes the victim feel powerless. The respondents in the study also explained that they experienced online harassment.

4.4 OnlineHarassment

The aspect of online harassment discussed in depth using eight of thesurvey questions asking respondents if when using the internet, someone sent pornographic or obscene images/messages, sent texts suggesting harm to them, their family,friends or property, exposed private information to others, pretended to be someone he/she is not, sabotaged reputation by spreading false rumors, sent other people's photos on the internet without approval, attempted to disable their computer by sending a virus or spamming.

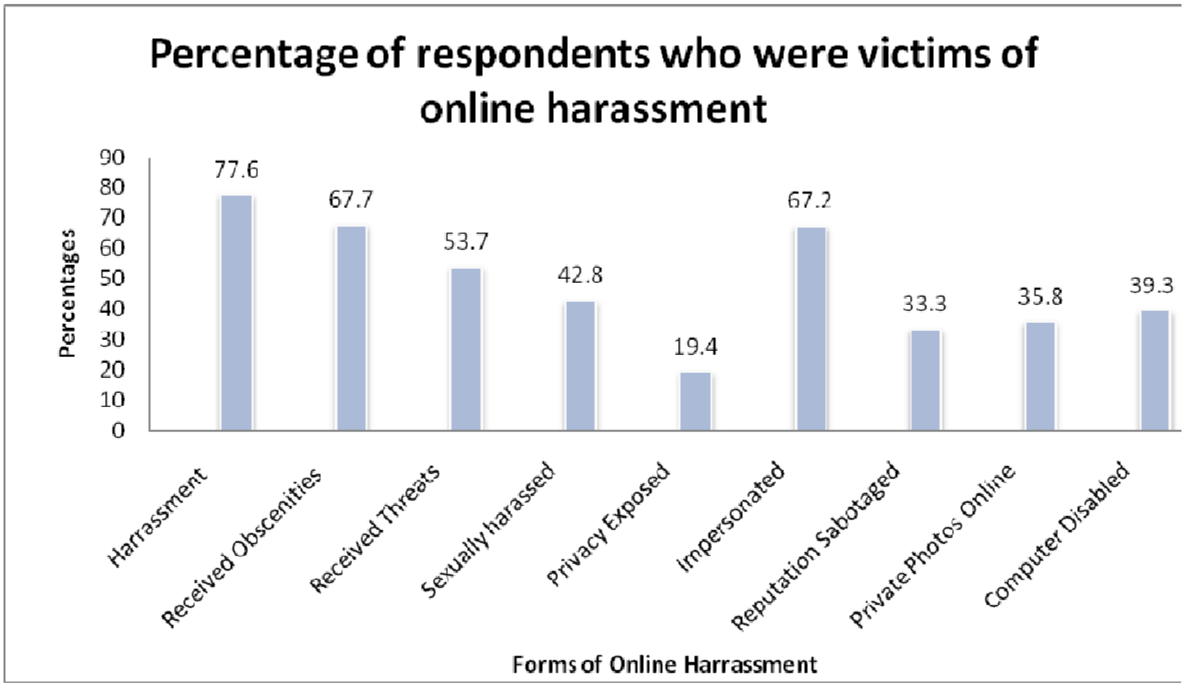
Each of the forms of online harassment was measured as (0 = No, 1 = Yes), representing whether or not the respondent had ever experienced any form of online harassment. Online harassment measure was coded as (0 = Never experienced online harassment, 1 = experienced at least one type of online harassment).Forexample,ifarespondentindicatedthey’ve hadtheir private photos posted online, they would be assigned a value of 1; likewise, someone who had also experienced all types of harassment would also be given a value of 1 and only those respondentswhodidnotshareanyform of harassmentwereassignedascoreof0.

Figure 4.3.1 above illustrates the lifetime widespread presence of cybercrime across the online delinquencies. Among sampled members, 77.6% (109) of the respondents admitted to having feltharassedbyactivitiesonline.One of respondent'snarrationofonlineexperiencedepictsthelevel of torment and psychological torture that online delinquenciescause: In reacting to the researchers probing, the respondent added that

> *"Someone popped up in yahoo chat and said hi when I was online. We chatted casually for sometimeatfirst;then,wegottoberegularchatfriends.Weexchangedphonenumbers,andI revealed a lot of information on where I stay and what I do. He told me he was staying in Mombasa. After some time, he made sexual advances to me, and I told him that I have a boyfriend. That is when he started spamming me with sexual messages, and I asked him to stop.HenowevenSMSmeonmyphone.Iconductsomebusinessusingthephone, and it has been difficult to discard the phone number because I fear losing my lifeline asthe business provides for my other needs as a side hustle. I am now depressed as the guy tellsmethathecancatchmeinpersonandevenkillme.Ifheissohypnotized,he cangetmeasIhadtoldhimallaboutme.Thishasstressedme.Idon'twanttotellmy boyfriend because he is so jealous, and I fear his reaction if he notes that I speak with other menonline,especiallythatwealsofirstmetonline.Ihadsenthimafewphotosofmeinsome seductive poses, so if I told my boyfriend, he would never believe it was innocent. Now I stand threatened, and I fear this guy could do anything. Of late, he is mailing me pictures of nude girls without heads; I think I should report to the police, but I fear the police will not understand and blame me. This is affecting me, and I wonder if someone can help. I have decided not to read his emails, but what do I do with the phone? Somebody help!" (25 years old)*

The following are the varied forms of online harassment reported: 67.2% (94) of therespondentssaidthatsomeonehadopenedonlineaccountsusingtheirphotos,names, and personal details or a person known to them, impersonating them. Additionally, 33.3% (47) reported that their reputation had been attacked, having their photos posted without their permission or lying spread about them to others viaelectronicmeans.The study findings also show that 67.7% (95) of the respondents reported that when using the Internet, someone has sent them pornographic or obscene images or messages, 53.7% (75) received threatening written messages directed to them, their family/friends or property, 42.8% (60) received sexually harassing or threatening messages or pictures, 53.2% (78) of the respondents reported that people online had made sexual advances towards them. 19.4% (27) had their private information exposed to others, 33.3% (47) had their reputation sabotaged through false rumors about them spread via the internet. In comparison, 39.3% (55) reported that someone attempted to disable their computer by sending a virus or spam. Statistics ofwhat washypothesizedtobeharassmentgaveanonlineharassmentpercentageof78.5%.

Figure 2:Widespread presence of online harassment againstwomen



Besides online harassment, the respondents also indicated that they experienced cyberstalking, as demonstrated in the following subsection.

4.5 CyberStalking

The study findings show that 76.1% (107) of the study participants have been stalked online. The measure of Cyberstalking was if one experienced online harassment and whether at any onetime,aperson'sharassingonlineactivitycausedthemtofearforpersonalsafetyandifthe crime wasrepetitive.

The prevalence of Cyberstalking is evidenced by what one of the respondents narrated:

> *"Ihaveblockedherfrommysocialaccounts,butshemakesanonymousaccountsandchecks my updates. I think she even poses with the name of one of my friends online because I have removed all the names of the people I don't know, but she still gets all my updates. She says that my posts are controversial and immoral. I fear her stalking habits and therepercussion they would have on my life that I have accepted to stand sabotaged and blackmailed. I feelIshouldhavemorerightstoexpression. She is violating my privacy." (35 years old).*

The output to the measure of online harassment was compared with fear and escalationofthecrimetoestimatecyberstalking.Impersonation/identity theft was taken as a form of cyberstalking without subjecting it to the dichotomies of fear andrepetition.

Table6 belowshowsthepercentagesonyesresponsefromtherespondentswhileaskedwhether theywereharassedonline,whethertheharassmentcausedfearofpersonalsafety,andwhether theharassmentwasrepetitive,keymetricsonCyberstalking.

Table6Cyberstalking againstwomen

	Number of women	Percentage
Experienced cyberstalking	107	76.1

Not experienced cyberstalking	33	23.9

The majority (77.6%;109) of the respondents admitted to having felt harassed by activities online, while 50%(70)oftherespondentsexpressedfearoftheironlineinformationbeingusedtoharassthem bypeopletheyhadbeeninarelationshipwith.75.6%(106)reportedthata person's online action had made them fear for their personal safety at one time in their life. Repetition was recorded through 45.3% (63) of the respondents who reported having been contacted after theyaskedthepersontostop,and52.2%(73)ofrespondentsreportedhavingbeenharassed and that the harassment hadescalated.

The study found out that 76.1% (107) of the respondents were victims of Cyberstalking, which comprised the cumulative forms of online harassments that were repetitive and caused an individual to fear personal safety. Additionally, 50% (70) of the respondents expressed fear of their onlineinformationbeingusedtoharassthembypeopletheyhadbeeninarelationshipwith, while 75.6%(106)reportedthatatonetimeintheirlife,aperson'sonlineactionhadmadethemfear for their safety. On the other hand,45.3% (63) of the respondents were contacted after asking them to stop. Nonetheless,52.2% (73) of respondents reported having been harassed and that the harassment hadescalated.

Hence, the researcher sought to establish the cybercrime perpetrators from a gender perspective.

4.5.1 Cybercrime Perpetrator by Gender

The study found out that 84.4% (118) of the respondents reported having been harassed by men online, 2.7%(4) said that those who harassed them online were men, while 12.9% (18) of the respondents did not know the gender of the perpetrator. The study also shows that the perpetrators of cybercrimes are not necessarily men, as shown in the table 7 below.

Gender	**Respondents**	**%age**
Male	62	44.2%
Female	60	42,7%
Unknown	18	12.9%
Total	**140**	**100%**

4.6 Forms of cybercrimes experienced by women

Responding to the question of online delinquencies experienced, study participantsreported onlineharassmentandcyberstalkingastheformsofcybercrimes.Thestudymeasureon formsofonlineharassmentwasifwhenusingthe internetsomeonesentpornographicorobscene images or messages, sent written texts suggesting harm them, their family/friends or property, sent them sexually harassing or threatening messages or pictures, exposed private information to others, pretended to be someone he/she is not, sabotaged reputation by spreading false rumors, sent otherpeople's photos on the internet withoutapproval,attempted to spam or sending a virus to disable your computer. .

Anopenquestiononothercybercrimesthatmayhavebeenoverlookedinatdesignstage, 'Give any other cybercrime that is not included in the list above in the space provided below'gavethefollowingasformsofcybercrimesagainstthewomen:Sexual harassment, spamming, threats, bullying, blackmail, sabotage, stalking, intimidating messages, spreading rumors, subscribing victims to unwanted websites, posting confidential information about the victim in online dating and sex sites, impersonating, posting pornographic and nude pictures online, morphing photos, posting pictures online without the owner's approval, emotional harassment and general misinformation.

Theformslistedbyrespondentswerefoundtohavebeenfullyincorporatedinthepostulated surveyquestionstomeasurestatesofcybercrimes,whichwere'have you beenharassedonline, stalked online, received obscenities, received threats online, sexually harassed, privacy exposed, impersonated, reputation sabotaged, private photos posted online without their approval and computer disabled.' The cybercrimes where the online harassment was repetitive and caused fear pointed to cyberstalking.

Theresultsonformsofcybercrimebyproportionswerebelow,leadingtotheconclusion that iscyberstalkingandonlineharassmentaretheprimaryformsofcybercrimes.

4.7 Effects of cybercrimes onwomen

The majority,73.1%(102)oftherespondents,admittedthattheharassmenthadnegativelyaffectedthem ,as evidenced by the following respondent'sexperience:

> *'SomeonecreatedafakeaccountofmeonFacebookandafakeemail.Theywouldupdatethe information as if it was me updating. They had my personal information like my phone numbersandmylegitimateemailsasan alternate,whichtheyalsoputonthisfakeprofile.They have subscribed to porn services and online dating accounts that I started receiving strange obscene phone calls and emails. I felt so much distressed by impersonation, violation,anddefamation.TheyweremycompetitorsortheirsupportersasIwasvyingfora post back in College politics. The most annoying is that they scanned my posters' photo and put it on an ugly nude body of a grandmother and put it as the wall picture on the fake profile.Thatwallisfullofabuses,annoyancesthataffect me as a person, and I couldn't sleep and couldn't ignore it. I got to be the laughing stock of the college. I reported to Facebook,whoblockstheaccount,butthepersonrecreatesasimilaraccountwithsmall variations of my name. I decided to give up and never contested again for any other seat. (27 years old, intern)*

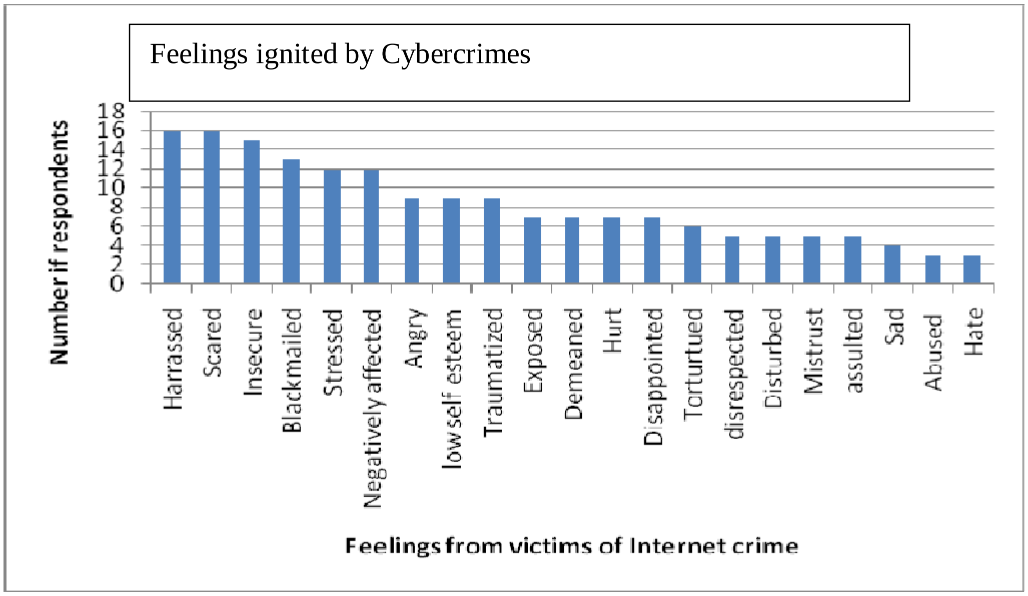
Some of the women commonly reported that cybercrimes annoyed and or tormented them emotionally, psychologically, or physically as evidenced by the respondent's experience,

> "*Someone hacked into my account, and they sent obscene messages to my friend's wall to date. It is very tormenting, embarrassing, and depressing. Some people on my friend's list are my aunties and uncles and my mother's friends who may not understand whathappens,orImayneverhavethechanceofexplainingwhathappenedtothem.Ifeltthis interferedwithmyreputationandspoiltmyname.It'ssohurting,disturbing,andIfeelthatit hasloweredmyself-esteem.Iwon'tusethe Internetagain." (39yearsold).*

These were online delinquencies that offended their human sensibilities hence qualify to be cybercrimes.

Women who reported to have been victims of various forms of Internet crimes which had affected them described how they were affected by the cybercrimes using the terms and magnitude shown in the diagram below:

Figure 3: Feelings expressed by victims of cybercrimes

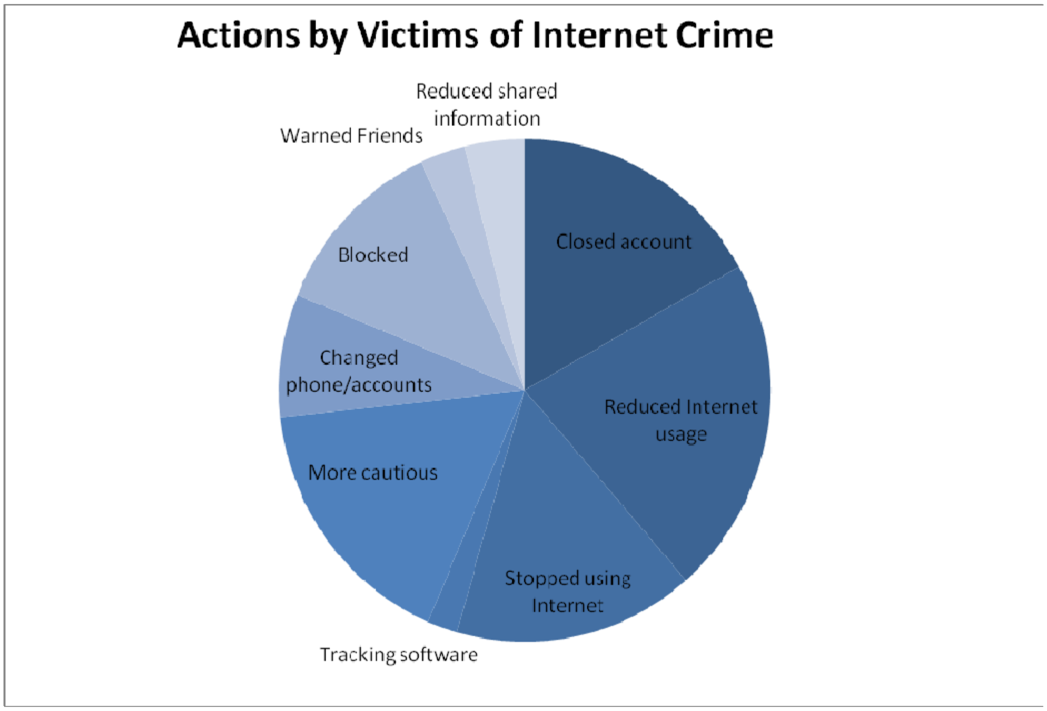


According to the study, 28 respondents out of the 140reportedhavingbeenattackedbypeopletheyfirstmetonline.Most of them were verbal abuse, but three women reported more severe physical attackssaidtohavebeenphysicallyinjuredbypersonstheyfirstmetonlineandlaterestablished physicalcontact.

One lady confessed that she was raped by a person she first met online and established a relationship,theotherwasslappedinasimilarcircumstance,andthethirdsaidshehaslocked up a room for days then released. She did not know what the man's motive was. During the study, 48.8% (68) of the women had been threatened with physical harm by a person they first interacted with online. In comparison,38.8% (54) of the respondents reported having flirted online to hookup,whichresultsinan offline physicalrelationshipfromonlinecontacts,makingonline contact just not virtual but real. However, 32.8% (46) of the respondents admitted to having hooked up withpeopletheymetonline,with10respondentsreportingthatthepeopletheymetonlineare their current husbands. Additionally, 53.2% (74) of the respondents had met people in person who they firstmetonline.Thewomenreportedhavingreacted,asshownbelow,followingtheattacks.

The researcher asked the respondents to explain the measures they took against cybercrime attacks.Thewomen's reactionsareshown in figure 4 below:

Figure 4 Measures taken by victims to mitigate or curbcybercrime



4.8 Risk factors associated with cyberCrime

Itwastheorizedthathaving many online activities mightexpose individual to cybercrime. The results indicate that those with many social networks or blogs and spend most of their time online were more likely to fall victims of cybercrimes. Therisk factors were analyzed in four broad categories: online exposure with regards to how much time one spends online, online guardianship looking at privacy settings, online proximity accepting friend requests from strangers, andtarget attractiveness using the type of information one posts online.

4.8.1 OnlineExposure

Theonline exposure conceptwasinvestigated in depth usingsixofthesurveyquestionsasking respondents how much time they spent online, what activities they engaged in while online and what information they gave out about themselves and how many social networks/blogsthey have. The study shows that 16.4% (23) of the respondents update their profile regularly, and only 1% (2)who reported not to update their profile at all; on average, each respondent has posted 160 personal photos, with the highest respondent having 640 private pictures on their face. However, 14.9% (21) of the respondents reported having spent more than 20 hours per week onsocial networksandblog,14.4%(20)spent10-20hours,25.9%(36)spent5-10hours,and44.8%(63)spent15hours.Norespondentreportedhavingpaidlessthananhourona socialnetwork blog. On inquiry of what women use the Internet for, only 29.4% of the total Internet use time was used for the study; the rest was used for social activities such as chatting, social networks, blogs, and instantmessaging.

4.8.2 OnlineGuardianship

This was measured by asking respondents if they used online profile trackers designed to monitor who is viewing their information and by asking if they had their online social network accounts set to limited or private access for purposes of restricting who viewed the students’ information posted on their online profiles. 68.2% (95) of the respondents had their accounts set to private, meaning that only persons accepted as friends can view the online information. In comparison,everyone on the Internet can view 31.8% (45) of the respondents’ data. 30.3% (42) of the respondents used a profile tracker to track who views their profile and what information they are considering. 56.7% (79) of the respondents took steps to protect themselves from blocking contacts and privacy settings.

4.8.3 OnlineProximity

This study set to determine whether the respondent has ever added a stranger as a friend on their onlinesocialnetwork.Mostoftherespondentshadnumerousfriends intheirsocialnetworkaccounts,most of whomarestrangers.Theaveragenumberofonline friends is 700, with the respondent with the highest number of online friends being 6800. 42.3%(59)reportedhavingbeenharassedbystrangers,while57.7%(81)oftherespondents had been in a previous relationship with theharasser.

Table 3Online proximity variables by harassment prevalence.

		Have you been harassed online?		
		Yes	No	Total
Information Online	First Name	50	17	67
	Full Name	45	21	66
	Relationship Status	88	11	99
	Sexual Orientation	28	1	29
	Email Address	75	18	87
	Interests/Activities	65	19	84
	Photos	91	9	100
	Address for Other Social Network/Blog Sites	6	3	9

4.8.4 TargetAttractiveness

This study utilized nine indicators of target attractiveness based on the type of information respondents may have posted/provided on their online profiles (i.e., online social network, blog),includingtheirfullname,theirrelationshipstatus,theirsexualorientation,theiremail address, address for another social network/blog sites, interests and activities, photos, and videos. The results are shown in Table 6 below.

Table 9:List of information posted on women'sonline profile and percentages

Information Online	Number of Women	Percentage
First Name	9	6.6%
Full Name	9	6.6%
Nickname	7	4.9%
Birth Date	13	9.6%
Relationship Status	12	8.4%
Sexual Orientation	5	3.3%
Home Town	10	7.4%
School address	2	1.6%
Home Address	2	1.6%
Job Title	3	1.8%
Work Name	10	.7%
Work Address	6	.4%
Email Address	12	8.8%
Home Phone Number	8	.6%
Cell Phone Number	5	3.8%

School Name	8	5.6%
Academic Course	7	5.2%
Clubs/Organizations	2	1.5%
Interests/Activities	11	7.7%
Photos	13	9.2%
Videos	2	1.6%
Top Friends	4	2.8%
Address for Other Social Network/ Blog Sites	6	.4%
Other	1	.1%
Total		100.0%

The above table shows the information reported to have been provided online by the respondents. A narrative by one of the study participants demonstrates how the information provided online could make one an attractive and reachable target:

> “*My current boyfriend first saw me online and sent me a ‘Friend Request.’ I accepted his request even if, by then, it was just another stranger. I add everybody who seems niceorwhorequesttobecountedasafriend.Wemetin ahoteloneday for coffee. When we became friends, he revealed that when he saw me online, he liked me. He frequently looked and checked at my profile and timeline for daily updates. This guy stalked me without my knowledge until I noticed him as he often liked and reacted to my updates/posts. I would receive messages on my phone from a secret admirer. Our friendship picked.He once revealed he watched me swim at an individual swimming pool in one of the hotels in town because I used to update my profileinthatswimming pool.Iliketheguyandamlookingforwardtomarryinghimafterfrequent meetups,but I thought it is dangerous to give information that can lead people to track you online to real life. I freak all the time when I think of what could have happened if he was a person of ill motive. I have since erased all the personal information on my Facebook, and I makesurethatallthatIputisgeneralinformation.” (32YearsOld)*

4.9 Summary of Findings

The mean age of the respondents is 32 years. The respondents enjoy 90% of Internet access in their homes, office/work, cell phones, Modems, and Cybercafe. Most of the respondents, 45% (63), were single. The married respondents experiencedhigher,64%(90),Internetstalking,andonlineharassmentpercentagesthanthesingle respondentswhoexperiencedonly36% (50) oftheharassment.The majority of the respondents reported usingthe Internet for social communication, with chartrooms, email, social networking sites, instant messaging, and blogs taking the highest percentage. At the same time, studies and work accounted for only 29.4% of total Internet usage. Cybercrimes were rampant, with 77.6% for online harassment and 76.1% for Cyberstalking. 73.1% (102) of the respondents admitted that the harassment had disturbed and negatively affectedthem.Cyberstalkingandonlineharassmentaretheprimaryformsof Cybercrimes. OtherformsofCybercrimewereidentifiedasreceivedobscenities,receivedthreatsonline, sexually harassed, privacy exposed, impersonated, reputation sabotaged, private photos postedonlinewithouttheirapproval,andcomputerdisabled.Alltheseotherformswerefound to annoy and or torment women and, hence, amount to online harassment making online harassmentandCyberstalkingthetwosignificantformsofCybercrime.

Women reported that Cybercrimes annoyed and or tormented them emotionally, psychologically. They stopped using the Internet after the harassment, reduced their use of the Internet, blocked accounts from harassers, and exercised more caution on the Internet, changed phones/accounts, and online identities. On risk factors for Cybercrime, some online activities were found to put individuals at more risk of cybercrime than others; those who have many social online accounts, update the statements frequently, especially with controversialtopics,isonlinemostofthetime,doesnotsettheirstoretolimitedtorestrict whoviewstheinformation,addsstrangerstofriendlist,andhaspostedpersonaldata on their profile are more at risk for becoming cybercrimevictims.

CHAPTER FIVE

5.0 DISCUSSION ANDCONCLUSION

5.1 Introduction

Several findings warrant discussion regarding the prevalence of Internet crimes on women and forms of Internet crimes. This chapter will discuss the majority of Cybercrimes,conditionsofCybercrimesexperiencedbywomen,effectsofCybercrimeonwomen, andriskfactorsthatincreasesusceptibilitytoCybercrimeonwomenbasedonthefindings in the previous chapter. It will give conclusions derived from the study, make recommendations, including suggestions for furtherstudies.

5.2 Prevalence of cybercrimesagainstwomen

Previous research outcomes show that women are more predisposed to cybercrimes as opposed to their male counterparts regardless of their relationship status.(Tjaden & Thoennes., 1998; Splitzberg & Hobbler., 2002). They all conclude that gender standsoutasapredictorofcybercrime.The study shows that most women use the Internet for social purposes, making them more susceptible to being victims of Cybercrimes than those using the Internet for research and official purposes. The majority of the respondents reported usingthe Internet for social communication, with chartrooms, email, social networking sites, instant messaging, and blogstakingthehighestpercentage. At the same time,studiesandworkaccountedforonly29.4%oftotal internetusage.Women are victims of cybercrimes, and the dangers of these crimes on women have been overlooked and affecting the optimal usage of this vital resource.

Outofalltherespondents,77.6%(109)werecybercrime victims;theyhadbeenstalked and harassed online. Women reported having been harassed online and stalked online. The otherformsofCybercrime,receivedobscenities,receivedthreatsonline,sexuallyharassed, privacy exposed, impersonated, reputation sabotaged, private photos posted online without their approval, and computer disabled; were broadly described as online harassment as findingshowstheyallmadewomenfeelharassed.Whereonlineharassmentcausedfearof personal safety and was repetitive, it amounted to Cyberstalking. Women reported that these crimes annoyed and or tormented them emotionally, psychologically, or physically as evidenced by the respondent’s experiences. These were online delinquencies that offended their human sensibilities hence qualify to be Cybercrimes.

The commonness of cybercrimes is evident but is absent from the plan of the feminist movement.WHOA(2010)ofvictims' characteristicsfindsthatvictims are predominantly female among users from 18-32. This study shows that respondents under 30 years of age experienced slightly more overall harassment thanthoseover 30 years (42.1% compared to 38.6%). This can be attributed to those below 30 years using theInternetmoreextensivelythanthoseabove30years.The majorityof thestudyparticipantswerebetween31– 40years,theaverageworkingage.

Internet crimes are discussed below in two broad categories:

5.2.1 OnlineHarassment

The widespread presence of online harassment was estimated to be 77.6%. A survey question asked directly, ‘have you been a victim of cyberbullying?’ was intended to determine if there is a discrepancy in what the women consideredharassmentandwhatwashypothesizedtobeharassment.

Statistics of what was hypothesized to be harassment gave an online harassment prevalence of 87.6% (123), while the respondent's response gave 77.6% (109). The discrepancy of10%showsthatsome online delinquencies were postulated to be harassing, but the respondent did not feel harassed by them. For example, 53.2% (74) of the respondents received sexually harassing advances, messages, or pictures, 42.8% (60) reported that people online had made sexual advances towards them, depicting that some did not consider the sexual advances as harassing. For reporting purposes, 77.6% (109) was used as this is what the respondents considered to be harassing.

5.2.2 CyberStalking

The prevalence of cyberstalking was estimated to be 76.1% (107). Cyberstalking means experiencing any one or many forms of online harassment (shown in Figure 4.4) on two or more occasions, which must cause fear of harm to an individual. Impersonation is qualitativelydifferentfromtheotherformsofcyberstalkingasitisnotnecessarilyacrime ofrepeatedstalkinganddoesnothavetocausefeartoqualifyforcyberstalking.Previous research (Bocij, 2003) had suggested that impersonation, such as identity theft is a form of cyberstalking. The UN REPORT 2006 estimated that aggressive behavior, harassment, abusive language, and demeaning images in online spaces areaimedatwomenandcomefrompartners either current or former.Spender also assumes it is only men who perpetrate Cybercrime while addressing a specific form of harassment known as flaming. However from the findings, the perpetrators of cybercrimes are not necessarily men as women were found to perpetuate the crime on fellow women too. The study findings show that 44.2% (62) of perpetrators of Cybercrime were men, 42.7% (60) were women, while 12.9% (18) of the respondents did not know the gender of the perpetrator. Those who are married are victimized more often than are single people. Nearly 44% of those in a relationship have been harassed or stalked online, compared to 36.8% of those available, widowed, divorced, or separated, indicatingthatdatingpartners,relatives,oracquaintancesmayberesponsibleforaportion of the stalking.

5.3 Forms of cybercrimes experienced by women

According to Duggal (2002), cybercrime is a criminal activity committed online and is divided into 3 major categories, a crime against humanity, against belongings, crime against the state This research focused on cybercrime against the person, specifically the women. For purposes of this research, cybercrimes are online delinquencies that affect the person and specifically those involving the woman. Cybercrimes affecting the person are child pornography, online harassment, and cyberstalking. Those that specifically affect women are online harassment and cyberstalking.

Findings show that online harassment and cyberstalking are the primary forms of cybercrimes that affect women's occurrence percentage. When respondents who were victims of all forms of online delinquencies were asked whether they were harassed online,alltheotheronlineoversights;receivingobscenities,onlinethreats,onlinesexual harassment, privacy exposure, online impersonation, sabotage of reputation, private photos posted online without consent and disabling computer; all were found to amount to online harassment.Thisconcludes that all these other forms of cybercrime amounted to online harassment in general. These crimes cause fear and are repetitive. They amount to cyberstalking.

All online delinquencies fell under online harassment; being cybercrime that offends womensensibilities(annoyandortormentoneormorewomenemotionally,psychologically, or physically) viaelectronicmeanswhich causesfearofpersonalsafety.

5.4 Effects of cybercrimes on women

Scottetal.(2001:12)arguedthatwomenfeltsaferstaying away from the internet as it was dangerous which furtherexcluded them fromfully participatingontheinternet hense denying them a chance to secure equalparticipation.

Cybercrimes harm women. They affect how women continue to utilize internetresourcesaftertheyortheiracquaintanceshavefallenvictimtoCybercrimes.Asa result of Cybercrime, women reported having been annoyed and tormented emotionally, psychologically, and physically. This trauma impacted their life and, consequently, their degree of internetuse.

An indication of how Cybercrime can affect life is evidenced by a student who gave her experiencestatingthattheonlineharassmentisthreateningtoaffectherbusiness,whichis part of her sourceoflivelihood,itcouldjeopardizehersocialrelationship,herlifeisthreatened, it'saffectingheractivitiesduetostress. Ithasalreadyimpactedheruseofthe internet.

The finding shows that most women who fell victim to Cybercrimes minimized using the internetorstoppedusingthe internetaltogether.Womenshouldnotavoidexploitingtheinternet for communication and access to information, including all online interactions,which discourages an already vulnerable group from participation, further marginalizing them and widening the digital gap. Women should be at the forefront of utilizing Internet resources for their social, political, and economic well-being.

Other female victims of cybercrime reported having changed online identities that disorientated and consequently led to minimizing internet usage through the loss of contact or became more cautious when using the internet, which interfered with and decreased their online communication and online access information.Their reaction to cybercrime negatively impacted the use of the internet as a critical resource toward seeking the empowerment course whose consequences are further marginalization. The implications of the women reaction after being Cybercrime victims further marginalizes,promotesdiscrimination,andalsowidensthedigitalgapasexplainedbelow:

Decreasing the frequency of internet use or completely stopping the use of the internet makes women not benefit from internet resource as an essential information reservoir where women can freely exercisetheir basic human rightsandaddressgenderinequalitiesthroughmovementsandcommunitiesagainst issues retrogressive towomen.

Blocking email accounts and social networks makes the women lose important contacts and essential information channels and also the information reservoir that the email is.

Changinginternetidentitymakesessentialpeopleorpeoplewithcrucialinformationnotget the women’s contact when required. A lady reported that a former supervisor informed her thathewaslookingforhervacation job placement contactsbutmissedherconnections.She hadchangedallhercommunicationchannelsowing toonlineharassment.

Some women stop to follow a worthy cause to distract online attention and reduce personal distress. An intern who gave their life story narrated that she stopped contesting for astudentorganizationpostfollowingtheabuse,defamation,annoyances,and slanderonherperpetuallyhackedsocialnetworkprofile.Shecouldnotcopewith theonlinelibel,soshesteppeddownowingto theonlineproblems.Thisshowsthatonline harassment could also influence women's placement in leadership positions, further marginalizingthem.

Many may trivialize online harassment and stalking, but online contacts were found to have translated to physical online communication from this research's finding. Therefore, apart from the injury to human sensibilities, online contact can also translate to physical harm.

Familiarity with the internet and its virtual nature causes internet users to think that such interaction is not dangerous and hence they cannot be attacked. But the reality, as seen in the findings, is that onlinecontactssometimesendupinreal-lifecommunications,leadingtoactualphysicalharmthatcauseemotionalandpsychologicaltrauma which might end up being longterm effects to the victim.Theresearchshowsrape,abduction,andphysicalbeatingfromthe first mere onlinecontacts.

When offenders use online resources against women, they further dangerous and more discriminatory agenda. But Cybercrime should not hinder Internet usage and should not discourage women from access to the internet as it just marginalizes them further. Women end up using the meager financial resources that could be used to mitigate this crime and seek assistance, e.g., counseling after falling victims, which would otherwise have been used for their development.

5.5 Risk Factors associated with an increase in cybercrimes against women.

To understand what exposes individuals to risk, the researcher considered online exposure, safety, attractiveness, and proximity in internet use. The study resultsshow that the more social networks on has, the more personal information and updates one gives and lackofuseonlineprivacysettings(i.e.,limited/private settings) are significant predictors of onlinestalking/harassment.

5.5.1 OnlineExposure

Online exposure is associated with increase in cybercrime as shown from the findings where the more online social networks one hadand the number of daily updates one gave on these networks exposed them to cybercrime. Chat facilities e.g., mobile phones used to send a text back and forth in social networks increased the risk of harassment and stalking. The ease of communication allowed by chat make various online delinquencies a simple task forthosewhotargetwomen.Social networks showing whether a person is online or not can also facilitate online pursuit and this could be one of the reasonswhy social networks are asignificantandpositivepredictorofonlineharassmentandcyberstalking. The more time one spends online and photos or videos posted online were also associated with exposure to online harassment and cyberstalking.

5.5.2 OnlineGuardianship

Security features including presense of firewalls and antivirus software on computers were made to safeguardusers against malicious software damage. The aspect of online guardianship was determined by whether the respondent accountshad privacy settings to control who had access to their information. Privacy settings reduces chances of the internet user falling prey to cybercrime. Respondents using a profile tracker reported higher harassment than those not using a profile tracker,depictingthateitheritdoesnotprotectvictimsfromcybercrimeormostmayhave installed a tracker after being victims as many respondents were reactive, not proactive in guarding themselves. Most reported having used measures to protect themselves after being harassed online, or one of their acquaintances had fallen victim tothesame.The study findings show that 30.3%(44)oftherespondentshad aprofiletracker to keep tabs on who is viewing their profile and what information they are viewing, while 69.7% (101) of the respondents did not, meaning they are not aware of who accesses their knowledge,theirfrequencyofaccesstoidentifyanyriskytrends.

5.5.3 OnlineProximity

Study findings showed that adding strangers as friends online potentially exposed users and increased levels of cybercrime. It increasedthelevelsofcybercrime with 42.3%(62)reportedhavingbeenharassedbystrangers, while57.7%(84)oftherespondentshadbeeninapreviousrelationshipwiththeharasser.

As indicated in a respondent’s narrative, if a cyberstalker is comes across a profile picture of someone he/she finds attractive, they send a friend request to that person and if thetargetaccepts,thatstalkercannowview,access,or downloadanythingthatthevictimhaspostedontheironlineprofile.Thisenablesthestalker toseethe activities the person is engaging in and in the process get information that would be useful in pursuing and becoming more attached to the victim for example, whattheyaregoingtodothatday,what their contact information is if the victim has listed it online, whattheir interests are, their relationship status etc.

5.5.4 TargetAttractiveness

Cohen et al. (1981: 508), stated that online attractiveness is the material or symbolic desirability of persons or property targets to potential offenders and anyonlineinformationthatfacilitatesthewomen's pursuitmakes the target more attractive to cyberstalkers.

From the study findings, online target attractiveness was associated with cybercrimes in that individuals who provided more personally-identifying information were harassed,meaningitmadeiteasierforcyberstalkerstocontactvictimsastheygottobemore attractive targets. The data reported to have been provided by the respondents onthe internet, which could be misused, is massive (Listed in table4.6).

In summary, based on the results presented, certain demographic groups are disproportionately victimsofcybercrime,andcertain online activitiesputindividualsatriskof being victims; Those who have many social online accounts update the statements frequently, especially with controversial topics, is online most of the time, does not set their account to limited to restrict who views the information, adds strangers to friend list, and has posted personal data including their full name, relationship status, sexual orientation, their addresses, hobbies, photos, and videos were at a higher risk of becoming victims of cybercrime.

5.6 Conclusion

Cybercrimes are common amongst women with online harassment 77.6% and cyberstalking 76.1% being the most common during the research period. This suggests that online harassment and cyberstalking is likely to increase with the growth of technologies that facilitate cybercrime. Thus,there is need for law enforcement agencies to implement the Laws that have been put in place.

Womenalsoneedtobeawareofonlineactivitiesthatputthematriskofvictimization, avoidthem,andbemorecautiouswhennavigatingcyberresourcesfortheirdevelopment.Thisstudy soughtinformationfrom what happens within the cyber space and the study findings indicate that as much as the internet offers opportunities for networking and participative democracy it has also been used for selfishmotivessuch as sexualharassment,hate,obsessionforlove, revenge, unhealthy competition, boosting ego and the desire to exert control over the victim to further dangerous and discriminatory agendas. Familiarity with the internetand its virtual nature makes users think that such interactions are not dangerous but in reality online communication has sometimes ended up in offline /face-to-face communication which has led to actual physical harm that cause longterm emotional and psychological trauma.

Laws of Kenya deals with cybercrime under the Computer Misuse and Cybercrimes Act, 2018 however the findings revealed that there are no adequate institutional policies and clear channels to report the crimes and seek assistance. As examined in this study, online harassment and cyberstalkinghaveharmfulconsequences,including victims' negative psychological and emotional responses.As a result, moreworkneeds to be done to measure, respond to, and understand theconsequencesofcybercrimes,especiallyonwomen.This will enable cybercrimelaws to address the issues based on empirical evidence. Cybercrime should nothinderwomen’sinternetusageandshouldnotdiscouragewomenfromaccesstothe internet as it just marginalizes them and widens the digital gapfurther.Thereisneed toraiseawarenessthrough capacity building for internet users to encourage onlineprotection proactively through civic education that includes clear direction on how to protectthemselvesagainstonlineperpetrators,vigorouscapacitybuildingtoletwomenknow how and what to do to navigate the internet safely.

5.7 Recommendations

5.7.1 Women using onlineresources

It is advisable for female internet users to make use of the privacy settings that are available to protect themwelves from cybercriminals and deflect unwanted communication attempts. They should also avoid posting personal information online. Reporting the inappropriate behaviors to web administratorsand serviceproviders,andthroughthesetgovernmentchannels.By taking all these precautions they will be making it more difficult for the harasser to commit the crime successfully. Internet users should avoid intentional agitation or threat to potential online harassers when unwanted communications arereceived.

5.7.2 Government and social mediaowners

The government should make the regulatory body (Communication Authority of Kenya (CAK), being the decision-maker who sets the agenda for internet providers and companies with websites), capacitated to regulate website contents and activities and monitor and block those who misuse theinternet.

The law enforcers to enforce and implement the The Computer Misuse and cybercrimes Act, 2018 to deal with cybercrime and train personnel from prosecution to judiciary to effectively deal with cybercrime.Those incharge of the online social sites should operationalizeavenues of reporting on misuse of theirwebsitesandmanagethereportseffectivelybypromptlywarning and even prosecutingthosemisusingthefacility.

The above three stakeholders should not fail in their supervision and protection responsibilities. They should collectively make it easier to report problem behaviors online like unwanted contacts/pursuits by promptly providing an online portal to act on the reports and improve surveillance of online environments by monitoringmisuse.They all should make Cybercrime prevention a priority and provide a code of conduct to siteusers.

5.7.3 Areas of furtherresearch.

i. Thesamplepopulation usedinthecurrentstudywasdrawnfromNairobi County. It would be beneficial to expand to other populations in other counties to understand betterwomen’s experiences with cybercrime.

ii. The data presented in the current study represent a single point in time. This study would benefit from obtaining longitudinal data (tracking the same sample at different points in time) so as to get comprehensive report on the women’s experiences with cybercrimes and the effects it has on their lives.

iii. A similar study should be carried out on a target male population to see if they would also encounter similar challenges as their female counterparts as this study has shown that women too can be perpetrators of cybercrime.

REFERENCES

Adam,A.,(2002).*InternetstalkingandInternetPornography:GenderandtheGaze,Ethics,and Information Technology*. New York: PalgraveMacmillan.

Ashcroft,J.,(2001).*StalkingandDomesticViolence.*Washington,DC:UnitedStatesDepartment ofJustice.

Babbie, E.,(1998). *The practice of social research.* London: Wadsworth.

Benerd,H.R.(1995).*Researchmethodsinanthropology.Qualitativeandquantitativeapproaches.*London: Altamira Press.

Bocij,P.,andMcFarlane,L.,(2003).Internetstalking:TheTechnologyOfHate.*PoliceJournal. 76, (3), pp.204-21.*

Bocij,P.,(2004).*InternetStalking:HarassmentintheInternetAgeandHowtoProtectYour Family.* Westport, CT: Greenwood PublishingGroup.

Brenner,S.,andGoodman,M.,(2002).TheEmergingConsensusonCriminalConductin Cyberspace. *UCLA Journal of Law & Technology, 2002, no.3.*

CentralIntelligenceAgency(2010).WorldFactbook2010-Kenya-Communications. Available at: https://www.cia.gov/library/publications/the-world-factbook/geos/ke.html.Retrieved on26/03/11.

Cochran, W.G.,(1963). *Sampling Techniques*. New York: John Wiley and Sons, Inc.

Cohen,L.E.,andFelson,M.,(1979).‘‘SocialChangeandCrimeRateTrends:ARoutineActivity Approach.’’ *American Sociological Local Review, vol. 44, pp.588-608.*

CommunicationsAuthority of Kenya(CAK),2011.QuarterlySectorStatisticsReport1st Quarter (July-Sept 2010/2011. Available at: http://www.cck.go.ke/resc/statistics/SECTOR_STATISTICS_REPORT_Q1_1011.pdf.

They were retrieved on 26/10/20.

Council of Europe, (2001). Convention on Internet crime. Available at:http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm.They were retrieved on 26/03/11.

DonnaHughes,(1997).*ProtectingWomenfromSexualExploitationviatheInternet.*NewYork : Routledge.

Duggal, P.,(2002). *Cyberlaw: The Indian Perspective.* Delhi: Saakshar Law Publications.

Ellison,L.,2001.*InternetStalking:TacklingHarassmentontheInternet.*Oxon:Routledge.

Ellison,L.,andAkdeniz,Y.(1998)Internet-stalking:theregulationofharassmentontheInternet. *CriminalLawReview,DecemberSpecialEdition:Crime.CriminalJusticeandtheInternet,pp 29-48.*

Elm,M.S.,andSunden,J.,(2007).*CyberfeminisminNorthernLights:DigitalMediaandGenderin a Nordic Context.* Cambridge: Cambridge ScholarsPublishing.

Felson, M. (2002). *Crime and everyday life (3rd Edition)*. Thousand Oaks, CA: Sage.

Finn, J., 2004. A Survey of Online harassment at a University Campus. *Journal of Interpersonal Violence. , Vol. 19, No. 4, April 2004, pp. 468-483.*

Furnell,S.,(2002).*Cybercrime:VandalizingtheInformationSociety*.Boston,MA:Addison- Wesley.

GraboskyP.N.andSmithR.(2001).“*TelecommunicationFraudintheDigitalAge*:The Convergence technologies.” New York:Routledge.

Greer,A.,(2007).‘MisogynyBaresitsTeethonthe

Internet.'SydneyMorningHerald,21August Available at http://www.smh.com.au/news/opinion/misogyny-bares-its-teeth-on-Internet/2007/08/20/1187462171087.html. Retrieved on26/10/20.

Harvey,D.,(2003).InternetStalkingandOnlineharassment:WhattheLawCanDo.NetSafeII: Society, Safety, and the Internet Conference Proceedings. Available at http://www.netsafe.org.nz/Doc_Library/netsafepapers_davidharvey_Internetstalking.pdf .They were retrieved on 26/10/20.

Herring,S.C.,(1999).TheRhetoricalDynamicsofGenderHarassmentOnline.*TheInformation Society, Vol. 15. No. 3, pp.151-168.*

Hindelang,M.J.,M.R.Gottfredson,andJ.Garofalo(1978).*Victimsofpersonalcrime:An empirical foundation for a theory of personal victimization.* Cambridge, MA: Ballinger PublishingCompany.

Hinduja,S.,andPatchin,J.W.,(2007).*SchoolClimateandCyber-Integrity:PreventingCyberbullying and Sexting One Classroom at a Time.* CA:Sage.

Israel,GlennD.,(1992).*SamplingtheEvidenceofExtensionProgramImpact.*ProgramEvaluation and Organizational Development, IFAS, University ofFlorida.

Jewkes,Y.,
(2002).*Dot.Cons:Crime,Deviance,andIdentityontheInternet.*Collumpton,England:
Willian.

Joseph,J.,(2002).*Internetstalking:AnInternationalPerspective.*Devon:Wil
lian. Kenya Communications Amendment Act(2009).
Lee,R., (1998).RomanticandElectronicStalkinginaCollegeContext.*TheWilliamandMary Journal of Women and Law, Vol. 4, pp373-466.*

Maxwell, A.,(2001). *Internet stalking*. Auckland University, Department of Psychology [Online]. Available at http://www.netsafe.org.nz/Doc_Library/Internetstalking.pdf. Retrieved on 26/10/20.

Miller, N.,(2001). *Stalking Laws and Implementation Practices: A National Review for Policymakers and Practitioners.* Institute for Law and Justice Available athttp://www.ilj.org/publications/docs/Stalking_Laws_Final_Report.pdf. Retrieved on26/10/20.

Ogilvie,E.,(2000).*Internetstalking.TrendsandIssuesinCrimeandCriminalJustice.No.166.* Canberra: Australian Institute of Criminology.

Sarkio,H.,2009.OnlineorOff,We'reAlwaysGirls":GenderedBehavioronanOnlineBulletin Board and Message Board Targeted at Girls. Paper presented at the InternationalCommunicationAssociation,SheratonNewYork,NewYorkCity.

Scott, A., L.Semmens, and L.Willoughby, (2001). *Women and the Internet: The Natural History of a Research Project.* New York: Routledge.

Smart,C.(1995).*Law,Crime,andSexuality:EssaysinFeminism.*ThousandOaks:Sage Publications.

Spender, D (1995). *Nattering on the Net.* North Melbourne: Spinifex Press.

Spitzberg, B., and Hoobler, G.,(2002). Internet stalking and the Technologies of Interpersonal Terrorism. *New Media Society, Vol. 4, No. 1, pp. 67-68.*

Taylor,RobertW.,ToryJ.,D.KallL.,EricJ.,andJohnL.(2006).*DigitalCrimeandDigital Terrorism.* NJ: Pearson PrenticeHall.

Thomas,D,andLoader,B.,(2000).*InternetCrime:LawEnforcement,Security,andSurveillan cein the Information Age.* London:Routledge.

Tjaden, P., and Thoennes, N.,(1998). *Stalking in America: Findings from the National Violence AgainstWomen.*Survey.NationalInstituteofJusticeCentersforDiseaseControlandPreventio n

ResearchBrief.Availableat:http://www.ncjrs.org/pdffiles/169592.pdf.Retrievedon26/10/20.

UnitedNations.(2006).The in-depthstudyonallformsofviolenceagainstwomen.ReportoftheSecretary-General. Available at: http://www.un.org/womenwatch/daw/vaw/violenceagainstwomenstudydoc.pdf. Retrieved on 26/10/20.

USAID-KENYA, 2007. E-Legislation Policy Development Initiative for the East African Community – Kenya Internet Law Model. Deliverable No. 6 – Final Report and Finale-LegislationPolicies.Availableat:http://pdf.usaid.gov/pdf_docs/PDACL263.pdf.Retrievedon 26/10/20.

Wall, D.,(2005). *The Internet as a Conduit for Criminal Activity.* Thousand Oaks, CA: Sage.

Wall,D.,(2007).*Internetcrime:TheTransformationofCrimeintheInformationAge.*Cambridge: Polity.

WebsiteforWorkingtoHaltingOnlineAbuse(WHOA),2011.*WHOA,ComparisonStatistics, 2010.*Availableat:http://www.haltabuse.org/resources/stats/2010Statistics.pdf.They were retrievedon 29/10/20.

Williams, M.,(2006). *Virtually Criminal.* New York: Routledge.

Wykes, M.,(2007b). *Internet-stalking and the media construction of crime.* Devon, England: Willan.

Wykes,M.(2007a).*ConstructingCrime:Culture,Stalking,Celebrity,andthe Internet.*Devon, England:Willan.

Yar,M.,(2006).*InternetcrimeandSociety.*ThousandOaks,California:SagePublicationsLtd.
Julious, S.A. (2009). *Sample Sizes for Clinical Trials*. Boca Raton: CRCPress.

Yamane, Taro. 1967. *Statistics, An Introductory Analysis*. New York: Harper and Row.

APPENDIX 1

Women's experiences with cybercrime

Questionnaire

I am kindly requesting you to participate in this survey examining women's experiences with cybercrime. As part of my M.A research, this survey will ask questions about your internet use and online social networks that you are in and the annoyances and dangersyouhaveencounteredonline.

Youwererandomlyselectedtoparticipateinthisresearchstudy,alongwith145otherfemale teachers. Your participation in this survey will take 10-15 minutes of your time and the responses will only be made to the researcher. Your identity will not be associatedwithyourresponsestopreserveyouranonymity.Kindly note that thereisnopayment or direct benefits to you forparticipation.

Thank you for your cooperation.

1. What isyourage? 18-30 31-40 41 orover
2. Marital status?:oSingle oMarried o Divorced oSeparated

   oWidowed
3. Where can you access the internet from? Tick all that apply.

   o SchoolLibrary

   o Home

   o PublicWireless

   o CellPhone

   o Staffroom

   o SchoolWireless

   oCyberCafé

   o Other, pleasespecify

4. How much time do you spend on the internet?

1-5hours 5-10hours 10-20hours 20+hours

5. What do you mostly use the internet for? (Please selecttwo)

Chatrooms □ Instantmessaging □

Email □ Study/Work □

Social Networking sites (such asFacebook)□ Other, pleasestate

6. Whatmode of communication do you frequently use ?

o Face-to-faceo OverthePhone oSocial networking sites oOther

7. What percentage of your contacts would you estimate frequently use some type of onlinecommunication?Example: wattsapp, Instant Messenger, Facebook, Twitter, emails 0 – 100 (increments of 5)

8. What percentage of your contacts would you estimate that you talk to online in an averageweek?

9. How many people do you have on your contact list on all your online social network/blogaccount(s)?

10. How many of your photos would you estimate that you have on your social network accounts?

11. Are any of your accountssettoprivateorlimitedaccess?

12. Haveyoueverusedaprofiletrackerthatkeepstrackofwhoviewsyour account? oYes oNo

13. Which of the following have you included on your social network/blog account(s)? (Please Check All ThatApply)

○ FirstName ○ o Full Name ○ o Nickname

○ Date of Birth Date ○ Relationship Status ○ Sexual Orientation

○ SchoolName

o TopFriends

o WorkName

o Residence

o School Address

o EmailAddress

o Interests/Activities

o Phone Number

o Photos

o Clubs/Organizations

o AddressforOtherSocialNetwork/Blogsite

o HomeAddress

o JobTitle

o Other, pleasespecify

14. On an average week, how often do you update information on your blog or social network account(s)? o 0–24 o 25 orMore

15. Hasanyoneevercontactedorattemptedtocontact you on more than one occasion even after you asked them to stop? GiveDetails.

16. Haveyouengaged with an acquaintance ora stranger with the intention or hope of pursuing a romantic or sexual relationship, including just hooking up? Give Details

17. Has someone you have had an intimate relationship with threatened or harassed you online? Explain

18. Hasanyoneeveropenedanaccountpretendingtobeyouoryouracquaintanceonline without yourpermission?

19. Hasanyoneyou met online evermadeunwanted sexualadvancestowardyouonmorethanoneoccasion?

20. Howmanysocialnetwork/blogaccountsdo you have? o 1–14o 15 orMore

21. Haveyoubeenharassedonline?Describefullyhowtheharassmentbegan.

22. Was the person who harassed you male or female?

23. Has anyone you met online threatened you with physical harm? If yes why?

24. Prior to the harassment did you have any relationship or contact with the harasser

online or offline? **Yes / No** If not, how do you think the perpetrator got your details? Explain youranswer.

25. When using the internet has someone:(answer yes orno)
    - i. Sent you pornographic or obscene images ormessages
    - ii. Sent you threatening written messages suggesting harm to you, your family/friends orproperty.
    - iii. Sent sensitive private information about you toothers without your consent.
    - iv. Pretended to be someone he/she isnot
    - v. Sabotaged your reputation by spreading false rumors aboutyou
    - vi. Sent photos of you on the Internet without yourapproval
    - vii. Attemptedtodisableyourcomputerbysendingavirusorspamming
26. Do you know why the person(s)is harassing you? Kindly give more details
27. How did the person(s) actions make you feel?
28. Have you been threatened with physical harm e.g rape, death, damage to property or harm to your loved ones?
29. Has your reputation ever been sabotaged by someone spreading false rumours about you, posting your photos without permission? **Yes / No**
30. Howwouldyousaytheharassmentaffectedyou?(yourfeelings)
31. Could you explain the impact? (e.g., stopped usingtheInternet).
32. In your opinion, what do you think should be done to protect internet users from cybercrimes?

If you have been harassed and you would like to share, please write about your experience, what exactly happened, your feelings, and the impact it had on you. It’s regretted that this had to happen to you.

Thank you for your cooperation