THE UNIVERSITY OF NAIROBI

SCHOOL OF COMPUTING AND INFORMATICS

Assessment of Awareness and Preparedness of Cyber cafe Internet Users to deal with threats of cyber crimes: A case of Nairobi County

PRESENTED BY: KING’ORI PETER MAINA

P56/60071/2011

SUPERVISOR: MR. S. RUHIU

MARCH 2014

A Research Project Submitted in Partial Fulfillment for the Award of Master of Science in Information Systems Degree of University of Nairobi

Table of Content

Declaration

I King'ori Peter Maina, declare that this research project is entirely my own work and where there is work or contribution of others it has been acknowledged. To the best of my knowledge, this research work has not been presented to any other education institution of similar purpose or forum.

Signature______________________________ Date_________________________________

King'ori Peter Maina

Reg. No: P56/60071/2011

This research has been submitted for examination with my approval as the university supervisor.

Signature__________________________________ Date____________________________

Samuel Ruhiu
School of Computing and Informatics
University of Nairobi

Abstract

The internet was originally designed as an open system for trustworthy users, yet with its rapid growth rate, it has become vulnerable to cyber crime. Awareness and Preparedness are considered key determinant of online behavior of internet end user. The online behavior in turn determine the frequency of cyber attacks an individual is likely to experience whenever he goes online. Unlike in the corporate world where there are policies, rules and regulations that governs how one is expected to behave when going online the same does not happen when we come to internet users within the general public. There are no rules governing how the general public accesses the net at homes or within cyber cafes. This makes members of the general public easy preys of cyber criminals. While much research has been undertaken in ways of promoting cyber security awareness among employees in organizations, very little has been done to promote the same awareness within the general public. At the same time as far as the researcher was able to ascertain very little research has been undertaken to gauge the level of awareness and preparedness in dealing with threats of computer crimes both within the general public and in the corporate world.

This study is a descriptive one that aims at assessing computer crime awareness and preparedness among computer end users in cyber café within Nairobi County in Kenya. A descriptive survey design was considered the most appropriate in this research since the researcher had no intention of influencing the outcome of the research. This study focuses on the internet users within the general public, and tries to determine the level of their awareness about cyber crimes and also their level of preparedness in dealing with threats of these crimes.

To assess both the level of awareness and preparedness among the internet users, a scale was developed using the various constructs that were adopted for purposes of data collection. The study reveals that very high levels of awareness and preparedness exist among the internet users within the country. But at the same time quite a large number of those who were surveyed took a neutral position in most the constructs that were being used to assess the level of awareness and preparedness; this might be a pointer to the fact that the level being deduced from our research using the scale developed might not be as high as being portrayed.

Dedication

I dedicate this work to my family for their unconditional support and love. To my late father Samuel King’ori Ruga who despite having never gone to school valued education above anything else. I owe the little education I have to Him.

Acknowledgement

I am grateful to Almighty God, who gave me the strength, courage, grace and all that I needed to accomplish this. My sincere appreciation goes to my Supervisor Mr. Samuel Ruhiu, for his endless support and guidance in the course of under taking this project. I also thank the MSc project assessment panel of Mr. Christopher A. Moturi and Mr. Evans Miriti who thoroughly and patiently scrutinized my work and gave their valuable contribution.

To my wife Tabitha Njeri and my children Richard, Mercy and Daysha thanks to you so much for the love, support and words of encouragement during this long journey; you were always there whenever I started losing heart. To my wife you remained a pillar of strength at all times in this journey. To my colleagues in the class of MSc 14 thanks for the support; special thanks to Titus Muhambe who believed that I was capable when I thought that it was impossible. To Juma Waithaka who took the trouble to make sure that I made sense out of the statistical measures.

Finally, I wish to extend my thanks to the management of all Cyber Cafés I visited for allowing me to conduct the study in their business premises.

Definition of terms

Awareness: Having knowledge of.

Combat: Fight against.

Computer: An electronic device for processing information and performing calculations

Crime: An act punishable by law; usually considered an evil act

Internet: A computer network consisting of a worldwide network of computer networks that use the TCP/IP network protocols to facilitate data transmission and exchange, also known as cyber space.

Preparedness: The state of being ready or willing to do something.

Security: The state of being free from danger or injury.

Ubiquitous: Seeming to be everywhere or in several places at the same time

Abbreviations

ACC: Attitude to risks of Computer crimes

CBD: Central Business District

CCK: Communication Commission of Kenya

DOS: Denial of Service

EAR: Exposure to Awareness Raising

FBI: Federal Bureau of Investigation

IDG: International Data Group

ICT: Information and Communication Technologies

KCC: Knowledge about Computer crimes

OB: Online Behavior

PR: Preparation to Respond

List of tables

List of figures

CHAPTER 1: INTRODUCTION

1.1 Background Information

The internet is evolving to be one of the most popular avenues for self – expression and social interactions (Prakash et al, 2013). According to IN VIA, a nongovernmental organization from Germany in its report of 2011, internet usage has become part and parcel of our everyday life and has thus fundamentally changed our habits as regards to information and communication. While developments in information and communication technologies (ICTs) have the potential to drive economic, social and political changes in a country; they also have the ability to advance criminal activities in any given country. Kenya as a nation has not been left behind in terms of internet penetration and usage especially via mobile phones (CCK 4th Quarter Report 2010 – 2011). The ICT infrastructure in Kenya has been undergoing rapid development, the arrival of undersea fiber optic cables in mid – 2009 being one of the highlights of this ICT infrastructure development; as a result of this development an upsurge of cybercrime activities in the country is bound to be observed.

The internet was originally designed as an open system for trustworthy users, yet with its rapid growth rate, it has become vulnerable to cyber crime (Lefebvre, 2012). This implies that Kenya as a country which is connected to the world wide net is not only prone to attacks by cyber criminals, but also a possible source of cyber crime activities. While most of cyber crime attacks might be targeting organizations; the internet users within the general public are also likely to become victims of the same or similar criminal activities. It is therefore important to asses both the awareness and preparedness level of internet users to deal with the threats of these criminal activities. We need to consider the fact that today; nobody is safe from confidential data theft and the accompanying fraud, which is accomplished using the stolen data. In the past individuals have always perceived themselves to be immune from cyber criminals activities; but today cases of people realizing that they have been victims occurs long after the crime was committed against them. This will normally from their bank statements or credit cards statements.

Forensic expert claims that cybercrime is costing Kenya about Kshs 36 millions every year; this is according to International Data Group (IDG) Connect report of 2013. At the same time the Federal Bureau of Investigation (FBI) Report of 2005 cited Kenya as one of the countries from which intrusions to American companies originated from. This implies that this country is a victim as well as a source or conduit of cyber crime activities.

Although cyber crime is often targeted at businesses and large organizations, internet use puts members of the general public at risk of cyber crime as well (LeFebvre, 2012). This should be a matter of concern to the policy makers. According to Ng (2010) individual computers users remains the weakest link within the security set up of any computer system. From a research done in United State of America by Ponemon Institute in 2010 lack of awareness about cyber threats among employees and user of internet is the number one cause of data breach in any given organization. The human side of computer security is easily exploited and constantly overlooked by security experts as well as the policy makers; as such user's awareness of the existing threats within information security set up cannot be understated. "As the general public browses the internet for information, shopping, and various other services, they create a network of connections that provides the opportunity for viruses to spread or other forms of attacks to occur" (LeFebvre, 2012).

To be able to develop appropriate policies and strategies of dealing with risks of computer crimes within the general public there is need to assess the level of awareness and preparedness among individual end users of the internet.

1.2 Problem Statement

Computer crimes contribute negatively to the development of any country by propagating various forms of frauds, child pornography, identity theft as well as intellectual property theft; thus there is need to assess the level of awareness and preparedness especially within the general public. As LeFebvre (2012) in her paper poses "does the general public have any awareness of the risk of cyber crime and are they willing or able to take protective action against these risks?"

This is implies that the first line of defense in any information security is the computer end user himself.

In order to deal with any form of crime the level of awareness about that particular crime need to be assessed first. This is given the fact that according to European Network and Information Security Agency (2006) awareness of the risk and available safeguards is the first line of defense for security of information systems and networks. According to Makatiani (2012) and Makumi (2012) many organizations in Kenya have automated their business processes, as such these organizations are now transacting most of their businesses online; these transactions ranges from paying of bills to applying for jobs. At the same time there are a lot of online financial transactions going on between individuals and individuals as well as between individuals and organizations; these includes mobile money transfer like Mpesa among others.

Mobile and online banking has become the norm rather than the exception within the financial institutions this country; while this has gone a long way in improving the speed of carrying out business the down side of it is that the incidences of computer crimes have increased.

From the forgoing it is very clear that there is need to undertake a study to assess the awareness and preparedness to deal with threats of cyber crimes among the internet end users. This is in order to be able to develop appropriate policies and strategies of dealing with threats of computer crimes especially within the general public.

1.3 Research Objectives

- To assess the awareness on the existence of computer crimes among individual internet end users in Nairobi, Kenya.
- To assess the preparedness in dealing with threats of computer crimes by internet end users in Nairobi, Kenya.
- To assess whether the awareness and preparedness in dealing with threats of computer crimes affect individual internet end users online behave.

1.4 Research question

The research will be guided by the following questions:

- What is the level of awareness about computer crimes among individual internet users in Nairobi?
- What is the level of preparedness in dealing with threats of computer crime in Nairobi among the individual internet users?
- How does the level of awareness about computer crimes and level of preparedness in dealing with threats of computer crimes affect the online behavior of internet end users in Nairobi?

1.5 Justification of the Study

Computer crime is real and in respects to certain offences an expanding phenomenon. This is taking into consideration that information whether personal or business related is becoming increasingly valuable to cyber criminals; the reason for this is that the information can be used for identity theft, credit card fraud or fraudulent withdrawal from a bank account among other cyber crimes (Smith, 2011). In order to be able to deal effectively with the threats of computer crimes, there is need to gain an understanding of the level of awareness among computer end users in Kenya about the existence of these crimes.

Despite several researches having been undertaken within the country dealing with cyber security and security of the information systems as deduced from the available literature (Makumi, 2012; Magutu, Ondimu & Ipu, 2011); it is clear to the researcher that very little study has been undertaken within the country to assess the level of awareness and preparedness about computer crimes for individual end user especially within the general public. That is very little research focusing on what the systems are being secured against has been undertaken within the country.

In the rise of Cyberspace a lot attention have been given to technical security, whereas on the contrary internet users might have been better served by more consideration being put to criminology. The study of crime in cyberspace has gained little support from the large information security industry (Thompson, 2002). This has created a problem in that the basis for drafting policies and strategies of dealing with threats of cyber crimes among the internet end users has become~~s~~ very difficult. To achieve any meaningful cyber security policies and strategies dealing with threats of cyber crimes targeting internet end user in this country there is need to determine the level of awareness and preparedness about these crimes within general public.

1.6 Significance of the Study

According to Olowu (2009) cyber-crimes are increasing within the African region due to the rapid growth of user base with poor security awareness and the lack of adequate regulations to govern this sector of the economy. The information generated in the course of this study will be important to policy makers since it will guide them when formulating policies and strategies affecting individual internet end users. The information generated in the course of study will also enrich the body of knowledge on cybercrimes in the country.

1.7 Scope of the Study

This research will be undertaken among people visiting cyber cafés within central business area of Nairobi County. The cyber café are used for this research considering that the people frequenting these places are all using computers and majority of them are also assumed that whatever business they will be transacting in the cyber café will be done online. These people are also presumed as being from different social background as well as having different levels of education. Thus they can be used as a representative of the general public internet end users.

1.8 Limitations of the Study

A lot research work has been done on information security within organizations. But from available literature very little has been done on issues of awareness about computer crimes especially among internet end users within the general public. For that reason chance of the people being interviewed and forming the sample population not being sure of what constitutes a cyber crime is very high. As Thompson (2002) in his paper poses “What do we really understand when we talk about computer crime?” This question is likely to be very relevant in this research in that when we come to the sample population the people being interviewed are likely not be within the cutting edge of ICT and as such might not be very conversant with what actually constitutes a computer crime. Therefore they might not be in a position to provide the most correct information that might be needed in order to draw conclusion. This is likely to constitute one of the limitations of this study. Another limitation of this research is that the individuals being targeted for the research might not provide truthful information; they might give information that they feel the researcher might be impressed with rather being truthful about what they actually know about computer crimes. This is considering that majority are not within the cutting edge of ICT.

Another limitation that we are likely to encounter in this study is that the cyber cafés from which the survey is being conducted are within an urban centre, thus it would be difficult to generalize our finding to the general population of internet users. By the virtue of the facts that these cyber cafes being targeted in our research are within the central business centre of Nairobi. Chances are that the majority of those frequenting these cyber cafés are likely to be more enlightened on issues of computer crimes than other cyber café users within the country; especially those in the rural areas.

1.9 Assumptions

One of the assumptions made in this research is that awareness and preparedness in a way affects the online behavior of the computer users; which in turn determine the frequency of computer crime incidences experienced by the user. The other assumption made is that there is a correlation between awareness levels and online behavior, as well as correlation between the respondent’s preparedness and their online behavior. The third assumption made is that there is a relation between online behavior and the number of computer crime incidences experienced by the internet user.

CHAPTER 2: LITERATURE REVIEW

Currently every effort is being made by the Kenyan government to ensure that most of it service can be accessed online; this is right from filing of tax returns to applying of government jobs; registration of students for national examinations as well as checking for national examination results (Directorate of e-Government Kenya, 2011). In essence the government has recognized that ICT is the next business frontier that requires to be leveraged in order to create employment. To take full advantage of this knowledge the government has a fully fledged ministry dealing with issues of ICT; at the same time it has earmarked land to put a techno city at Konza (Kenya ICT Board, 2012). All this is aimed at attracting both local and foreign investors to invest in the ICT sector. For the intended gains of these undertaking by the government to be attained issues of cyber crimes must be taken into account, and addressed.

Substantial amounts of research regarding computer crimes have been done globally, but in this country researches focusing purely on computer crime are not so significant. According to Magutu, Ondimu and Ipu (2011) no cybercrime research has been focused on this country; as such a lot need to be done on this front to ensure that information about computer crimes is readily available within the country.

2.1 Definition of computer crimes

Currently there is no universally accepted definition of computer cyber crime; this is because the crime covers an array of offenses. “One might not find the word ‘cyber-crime’ in contemporary lexicon, but it is a very popular term describing the criminal activities related to cyberspace or the cyber-world” (Olowu, 2009).The following are some of the definition used for computer crimes by different organizations:-

- US department of Justice defines Computer crime as "any violation of the criminal law that involves the knowledge of computer technology for its perpetration, investigation or prosecution" (Kunz & Wilson, 2004)
- According to Mathews computer crime is any crime that uses a computer and computer network as cited by Arpana and Chauhan (2012)
- Business Software Alliance classify computer crime as illegal activities that make use of electronic systems as a means to affect the security of the computer system and computer data, as cited by Kunz and Wilson (2004)
- Gordon and company define a computer crime as "the result of offenders perceiving opportunities to invade a computer systems to achieve criminal ends or use computer as instruments of crime, betting that the guardians do not possess the means or knowledge to prevent or detect the criminal act" (Gordon, Hosmer, Siedsma & Rebovich, 2003).

In order to deal with threats of computer crimes effectively it is important for this country to adopt a definition of computer crime that is in line with the ones commonly used by other countries.

2.2 Types of Computer crimes

Computer crimes fall into three basic categories according to Wall (2003); these are: - crimes related to the integrity of the computer, the computer itself and the content of the message from the computer. According to ITU Global Strategic Report of 2008 there are four different categories of computer crimes, which are:- Offences against confidentiality, integrity and availability of computer data and systems; Computer – related offences; Content – related offences; Offences related to infringements of copyright and related rights.

2.2.1 Crimes related to the integrity of the computer and its network

These are crimes basically dealing with issues of integrity of the computer or its systems and include hacking or cracking; this is the gaining of unlawful access into a computer system where ownership has already been established. These crimes basically have the computer or the computer system as the target as well as the means of the attack. Unauthorized use of a computer might involve stealing of username and password or might involve accessing the victim's computer remotely. The purpose of stealing of user name and password is to assist in the commission of further crimes. Another form of this type of crime is Denial of Service (DoS), normally achieved by hogging the available bandwidth thus denying the legitimate users the use of their bandwidth.

2.2.2 Crimes related to the computer itself

These are computer crimes that include various forms of computer frauds and theft that are perpetuated or made easier by means of a computer. These are traditional or existing crimes whose scope or form is transformed by use of internet. According to Wall (2003) they include intellectual property theft, online gambling, e-auction, phishing and various forms of frauds.

2.2.3 Crimes related to the content of message sent from the computer

These are crimes that have to do with the kind of content that is spread though the internet. In strict sense of the word these are also traditional crimes that have been made easier to accomplish by use of the internet. They include various types of pornography, cyber bullying, stalking and hate speech.

2.3 Reality of Cyber Crimes

Understanding cyber crime will guides us so as not to fall prey to specific cyber crimes such as identity theft and cyber fraud (Baiden, 2011). As every aspect of our daily life become deeply dependent on the Internet, we become prone to disruptive cyber attacks. These attacks can actually take various forms. To be able to deter and if possible prevent the commission of these crimes against individual internet users there is need to assess their levels of awareness and preparedness as far as computer crimes are concerned. Email is increasingly seen as the communication medium of choice amongst the technically aware population; the same group also considers communication to be the most important services on the internet; but unfortunately it is also the most insecure this is according to the report by IN VIA (2011). With the increase in mobile phones connectivity through which users can easily be able to go online and access their emails as well as visit social sites, an open window is offered to the criminal elements to exploit this opening since the awareness level about computer crime is likely to be very low or lacking altogether among the internet end users. According to Harrison (2013) the fastest way for criminal organizations to breach security is through e-mails.

As Gordon, Hosmer, Siedsma and Rebovich (2003) states "crime occurs when there is a suitable target, lack of capable guardians and motivated offender". The question we need to ask ourselves is does this scenario apply to Kenya? Are suitable targets for attack available? Are the guardians capable of dealing with computer crime perpetuators? Are there motivated offenders out there? There is need for us to be aware and prepared since the country is connected to the cyber space. We need to know that if we are not the target of the attack we can be the host of the crimes or attacks. This is given the fact that computers that have been compromised can be used by motivated hackers to launch attacks even when the attackers are not anywhere near the computer being used.

Information Communication Technology (ICT) is ubiquitous, supporting every industry sector, improving the capabilities and productivity of every business and providing benefits to every home and individuals (Anderson & Coffey, 2010). One of the phenomena of the ICT age is the constant threat of cyber attacks - malicious attacks against computers and computer users (Keren & Elazari**,** 2012). Traditional criminal behaviors are finding a new and a fast mode of commission as well as a wider scope, while new crimes are arising as a result of the innovations and advances in technology. Where we are heading too, computer crime is going to be considered an emergency very soon; the process of measuring awareness and preparedness to deal with emergencies is a very complex issue. The same is also true when dealing with computer crimes this is because of the ubiquitous nature of ICT.

Currently were are relying on technology to transact all kinds of business, from official to personal as well as socializing. "Our overreliance on the internet, e – mail, instant messaging, chat rooms and other communication technologies has made cybercrime a growing social problem that affects users everywhere and anywhere in the world"; this is according to Thapa & Kumar (2011). Baharudin (2007) avers that computer abuse incidences are increasing at an alarming rate despite organizations and countries efforts in implementing counter measures such as ICT security policies and appropriate technologies.

2.4 Dangers of Cyber Crimes

The Information Superhighway is undergoing rapid growth; as a result internet and other telecommunication technologies are making advances virtually in every aspect of the society throughout the world (Thapa & Kumar, 2011); this has fostered commerce, improved education, health care and promoted democracy in both developed and developing countries. At the same time means of communication (via internet) among family and friends has easily been facilitated. But the down side of this is that the same attributes that makes this technology an attractive medium of communication also attracts criminal elements especially due to its speed and anonymity. According Sandywell, cited by Koops (2011) this sense of anonymity of the internet makes it a very dangerous place to operate from, this is because some of the users are able to hide their identity while others feel secure hiding behind the Internet Protocol (IP) address. Thus one needs to be careful when going online, given the dangers that lurk out there. Apart from it speed and anonymity other factors also make cyberspace very dangerous include globalization as pointed out by Koops (2011). According to Yar, cited by Koops (2011) a cyber criminal can look for the most vulnerable machine or victim anywhere in the world, without leaving the security of his room; then use that machine to commit a crime. Due to the global reach of the internet, challenges of jurisdiction comes in, in that a person in Nigeria can commit a crime in Kenya, while still in Nigeria. Thus persecuting the perpetrator even when identified would require cooperation between the Kenyan government and the Nigerian government. This is very dangerous especially when the crime that has been committed in a given country is not deemed to be a crime in the country in which the perpetrator is operating from. Thus it becomes imperative for an individual to take precaution not to become a victim of cyber attack when going online, since the moment he becomes a victim chances of getting remedy or justices might proof to be a tall order.

“There will always be risk in cyber space; this risk is bound to grow as we become more dependent on software and computers” (Lewis, 2013). A minimum standard of due care need to be stated when it comes to cyber security. This will enable end user to take the bare minimum precautions when going on line. The internet is currently largely a lawless zone, a playground for a wide variety of undesirable activities, a paradise for all sorts of criminals.

According to Maybury (2009) “Hackers are troubles of our economy; but employees who use their computers to steal proprietary data or intellectual property also cause significant business losses”. This implies that computer crimes can also originate from within the organization rather than from outside. At the same time “most damage from cyber crime is likely to be caused by indifferent and or uninformed users of computer equipment and the internet” (Mesko & Bernik 2008). Cyber crimes are assumed to take place virtually and as such they have no effect in the real world, this tend to create a false sense of security that makes people to be a bit complacent when going on line. This ignorance by those internet users of the dangers lurking out there in the cyber space can cost an organization as well as the individual dearly.

2.5 Kenya in Cyber space

The Kenya government is working towards achieving a paperless civil service, through the implementation of e-government strategy. The challenge in this is that this has opened an opportunity for criminal element to gain access to information held online by government Institution; unless this information is safely secured.

In 1998 Kenya government amended it information act; the amendment enumerated various offenses with regards to data protection, unauthorized access to an information systems and data; unauthorized interception of computer services; damaging or denying access to a computer system; unauthorized modification of computer material; unauthorized access to a protected computer system (Murungi, 2012). These amendments were aimed at addressing issue arising from advances in technology and also in acknowledgement that Kenya is already a player in the cyberspace. With the launching of undersea cable the connectivity to the outside world is bound to improve, while communication through this medium is bound to affect the way we socialize as well as we transact business; criminal elements will also be able to up their game using the same medium. The need to be prepared to deal with challenges that are bound to increase with this improved connectivity is a must.

The cyberspace is defined by its ubiquitous connectivity; this tends to open up the space to the greatest risks (Schreier, Weekes & Winkler, 2013). Kenya is firmly within this connectivity and as such is bound to be a host, a target or perpetrator of the cyber crimes. A survey carried out by Federal Bureau of Investigation (FBI) of America in 2005 indicated that Kenya was one the countries from which intrusions to American companies originated from (Computer Crime Survey, 2005). Even though evidence of an intrusion from a particular country does not necessary mean that the intrusion originated from that country; but it implies that there is likelihood that some computers within that country have been compromised (botnets) and are thus being used as stepping stone to carry out the intrusions. Given that this was the position in 2005, it implies that the number of intrusion emanating from the country can only have increased. At the same time cyber crime activities target Kenyan institutions are also likely to have increased within the same period.

2.6 Kenya's effort to combat cybercrime

According to Business Daily (2013) Kenya stands the risk of becoming one of the world's major information security hotspots due to the general lack of awareness on existence of threats among the internet users, absence of a dedicated cyber security watchdog and legal framework. Computer-related crime is a long-established phenomenon, but the growth of global connectivity is inseparably tied to the development of contemporary cybercrime (UNODC, 2013). Kenya currently acknowledges the Budapest Convention and Commonwealth Model Law on cybercrimes even though it is not yet a signatory to the convention (Global Project on Cybercrime, 2013). Various activities reported in the media indicated that the country acknowledges that computer crimes are an issue in this country; and efforts are being made to address these issues. According to the Global Project on Cybercrime (2013), countries profile; Kenya is indicated to have enacted the Information and Communications Act 2009 , which criminalizes, unauthorized access to computer data, unauthorized access to and interception of computer services, unauthorized modification of computer material, damaging and denying access to computer system, unauthorized disclosure of password, unlawful possession of device and data, electronic fraud, tampering with computer source documents and publishing obscene information in electronic form. When viewed in totality this law is not adequate to address the challenges of computer crimes. In 2008 Kenya in collaboration with Global Project on Cybercrime organized a workshop on cybercrime legislation and investigation (Global Project on Cybercrime, 2013). The workshop is an indicator that cyber crimes or computer crimes is an issue in the country; and the country is collaborating with others to address the issue, but still more need to be done to arrest the situation. Kenya does not have sufficient legislative, policy and administrative measures mandating institutions as well as officials or individuals to secure and protect personal data (Sihanya, 2011).

The online world allows for anonymity because it is easy to fabricate IP addresses and destroy the evidence leading back to the hackers (News24, 2013). For this reason unless a country is well prepared it will be very difficult to deal with threats from cyberspace. A National Cyber-Security Steering Committee (NCSC) has been established to spearhead the war against cyber crime and related fraud in the county this is according to News24, Kenya; a national media house reporting on the proceeding of cyber security forum organized by CCK in 2013.

2. 7 Cyber Crime Awareness

Awareness allows the relationship between user's action or inaction and cybercrimes attacks or commission to become clear. The awareness makes it easier for the users and system administrators to be able to maintain and monitor an intrusion detection system that requires investigation. The first line of defense in cybercrime is users' awareness of the existing dangers or threats. From a research done in United States of America by Ponemon Institute in 2010 lack of awareness about cyber threats among employees and user of internet was pointed out as the number one cause of data breach in an organization. Informed internet users who can be able to recognize incidences of computer crime are more likely to be proactive rather than reactive when going online. An informed user is likely to unearth other situations that can decrease performance of a computer system and cost money; thus these situations can be dealt with before damage is caused.

The concept of computer crime awareness in this research is that the user is aware of various forms of computer crimes and their mitigations. An informed internet user will have a greater capacity to recognize and respond to risks of computer crimes.

Computer crime awareness will generally tend to increase knowledge and better computer practice by individual users of computers. “It is important for the management in an organization to obtain a feedback on user awareness of computer security practices in order to develop strategies towards ensuring the effectiveness of the policy” (Antwi-Bekoe & Nimako, 2012). Any organization that has a policy on use of the organization computer systems will once in a while require getting feedback on how well the end users of the systems are aware of the issues likely to compromise the organization computer systems; and how well they adhere to the policy.

2. 8 Cyber Preparedness

Cyber crime preparedness can be considered to be the ability of an individual to maximize his potential to deal with cyber threats while minimizing the cost that is bound to arise from a successive attack. Computer users should be pro- active when dealing with cyber threats rather than being re – active. They should be in a position to detect the threat before intrusion or occurrence of the event; being pro-active means that they have taken the necessary measures to safeguard themselves from cyber attacks by having the necessary knowledge and technologies to prevent the attacks or security breaches. They should have the necessary and appropriate tools as well as the correct procedure of deploying these tools in place. Thus in this research what we aim to find out is whether individual users have any awareness at all about computer crimes as well as whether they are prepared at all.

2:9 Computer crime as an Emergency

In most of developed countries many of the essential and emergency services rely on uninterrupted use of the Internet and communication systems; thus an attack on these structure considered critical to service delivery would be detrimental the nations security. This signifies that computer crime can rightfully lead to serious cases of emergencies. By understanding that computer crime poses a threat to the survival of nation state most countries have set up Computer Emergency Response Teams (CERT). Communication Commission of Kenya (CCK) was mandated by the Kenya Information and Communications Act CAP 411A to establish a national Computer Incident Response Team (CIRT) (www.cck.go.ke/industry/information_security/ke-cirt-cc/functions.html). "Military forces, faced with diminishing roles in preparation for large scale physical conflicts, have begun claiming that civilian cyberspace needs to be re – militarized and that the armed forces should be given both the technical tools and the legal rights to conduct not just cyber – defense activities but offensive cyber - attacks " (Adams, Reich & Weistein, 2012). This poses a new challenge for the civilian population in that if the military come in and they are allowed to have pre – emptive cyber attack capability the collateral damage is bound to be massive. As Emke (2008) quoted by Pladna (undated paper) points out, in the Spring of 2007 the State of Estonia took a whole month defending itself against denial of service attacks, mostly affecting its banking system; these attacks originated from Russia but utilized bots located all over the world. Even though Estonia is one of the most developed countries in Europe with ubiquitous usage of information and communication technology in all areas of life the attack brought its IT infrastructure to a standstill (Aslanoglu & Tekir, 2012). Tikk (2008) quoted by Aslanoglu & Tekir (2012) pointed out that in August of 2008, Russia launched cyber attacks against a large number of Georgian government websites, making this the first case in which international political and military conflicts was accompanied by coordinated cyber conflict. The damage caused by these attacks was massive. If Kenya was to face this kind of attack how would the country fare? In January 12th, 2010 Google publicly disclosed that they were under highly sophisticated and targeted attack on their corporate infrastructure originating from China (Aslanoglu & Tekir, 2012). These attacks resulted in theft of intellectual property from Google and access of Gmail accounts of Chinese dissidents; this attack known as Operation Aurora was against software exploited vulnerability and was accomplished without the internet users' awareness. In June, 2010, Stuxnet worm, which was unprecedented sophisticated attack targeting

Programmable Control Logic (PLC), was discovered (Aslanoglu & Tekir, 2012). The Stuxnet worm sabotaged Iranian nuclear centrifuges (Jellenc, 2012). The worm infected the concerned machines via Universal Serial Bus (USB). According to Miyachi (2011) quoted by Aslanoglu and Tekir (2012), before the worm came into the picture there was a lot of faith in the safety of the control systems since the USB was used for data transfer without any internet connection, and thus virus would be monitored. All these case indicates that cybercrime has the potential of leading to very serious emergencies not only affecting individual users of the internet but national state security.

An important component of safety in cyberspace is that individuals are aware of the risks they are exposed to and as such need to take actions to mitigate and/or prepare for such emergencies. As Enders (2001) point's out the task of increasing community preparedness for emergencies involves effecting a behavior change. Thus any framework developed to address preparedness has to deal with how an individual moves through the behavior change process. It has to deal with how they receive the information about the risk, how they perceive the risk and how they behave in relation to the said risk. This is based on the believe that once an individual has the necessary information he will act accordingly; but unfortunately there are several steps between an individual receiving information and changing his behavior as pointed out by Nielsen and Lidstone in 1998 quoted by Enders (2001).

The process of measuring emergency awareness and preparedness of the community is very complex (Enders, 2001). Taking the same line it can be urged that the process of measuring the level of awareness and the degree of preparedness to deal with cyber crime is bound to be a very complex affair; since like other emergencies it involves a behavior change. In order to overcome the complexity involved a survey need to be carried out, but it is important to identify what goes into the survey and who is targeted in this survey, this according to Enders (2001). The same argument can be applied when we come to cyber crimes. In this case there is need to clarify who is a computer/ internet end user. At the same time there is need to consider what is considered as acceptable level of awareness when we come to computer crimes; this should not be reduced simply to the general knowledge about computer crime but it should also include knowledge of the underlying risks of computer crimes. When we come to preparedness we need identify what can be considered to be an acceptable degree of preparedness; this should include steps necessary to safeguard one against likely threats and risks.

In this research the desire is to determine the level of awareness as well as degree of preparedness in dealing with cyber crimes since this will eventually inform policy decisions in any organization or a country.

When an individual is exposed to information pertaining to certain risks he can choose to use that information or not to use it. This forms the first step in awareness creation; this is normally affected by the attitude of the individual. This is because attitude will influence the kind of information an individual seeks and retains as well as the manner in which this information is understood this is according to Eiser et al (1994) as quoted by Enders (2001). Basically several factors influences awareness and behavior change process; thus the process of measuring awareness level should take care of these factors. When it comes to preparedness as pointed out by Johnson et al (1999) and quoted by Enders (2001) several factor need to be taken into consideration when it is being determined. These factors include perceived risk, amount of relevant information available, level of knowledge about the threat and hazard related variables among others.

A holistic framework for looking at awareness and preparedness has been developed seeking to clarify the factors that need to be considered in order conceptualize the issue relating to awareness and preparedness (Enders, 2001). Figure 1 below represents the proposed framework which was designed to address general emergency issues. By using this framework as a base; a framework that can be used for cyber crime awareness and preparedness assessment can be developed.

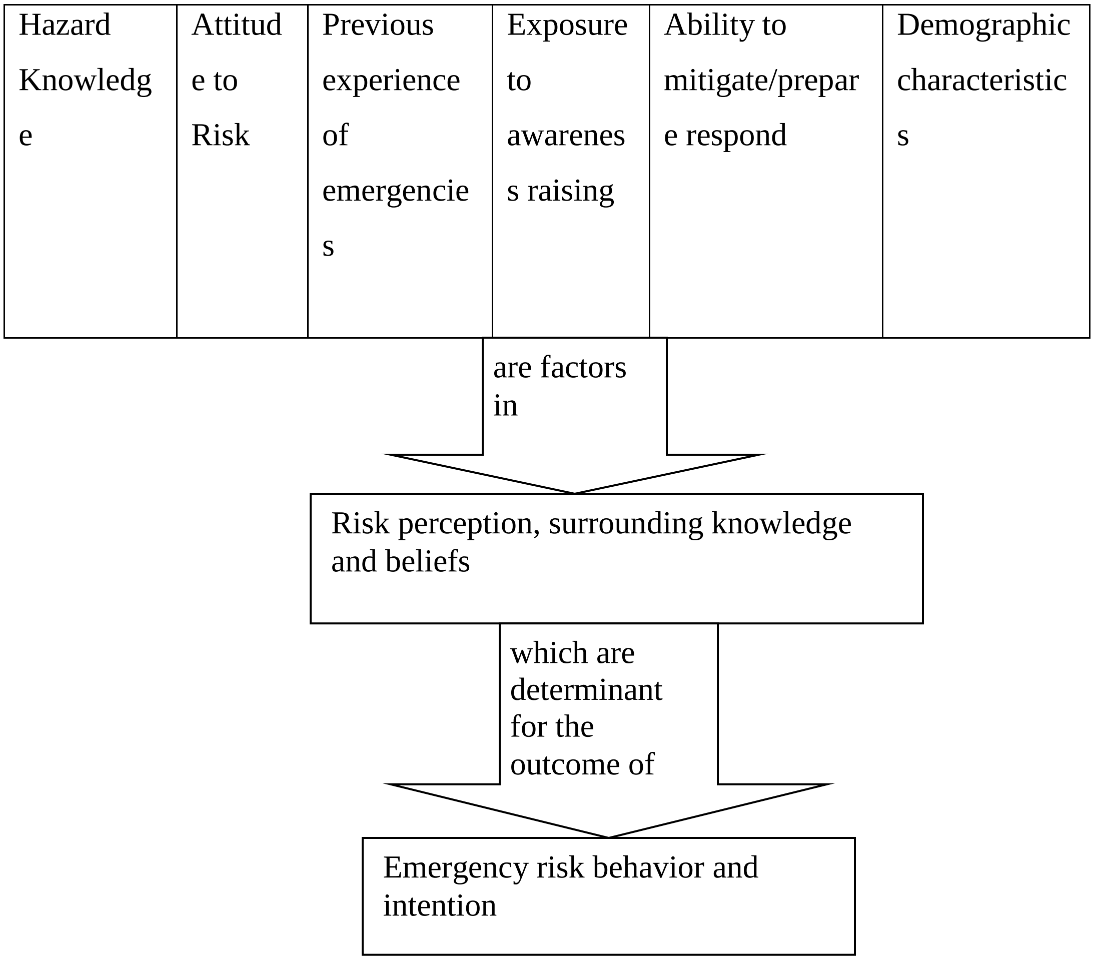
Hazard Knowledge
Attitude to Risk
Previous experience of emergencies
Exposure to awareness raising
Ability to mitigate/prepare respond
Demographic characteristics
are factors in
Risk perception, surrounding knowledge and beliefs
which are determinant for the outcome of
Emergency risk behavior and intention

Figure 1: Framework for investigating emergency awareness and preparedness (Enders 2001).

The above framework was adapted to suit computer crime**.** It was translated into a set of research questions that were used as data collection tool. For this framework to be of use in our research the factor mentioned were replaced by computer crime related factors. For example risk behavior in the generic framework was replaced by online behaviors; since online behaviors are bound to expose an individual to computer crime threats.

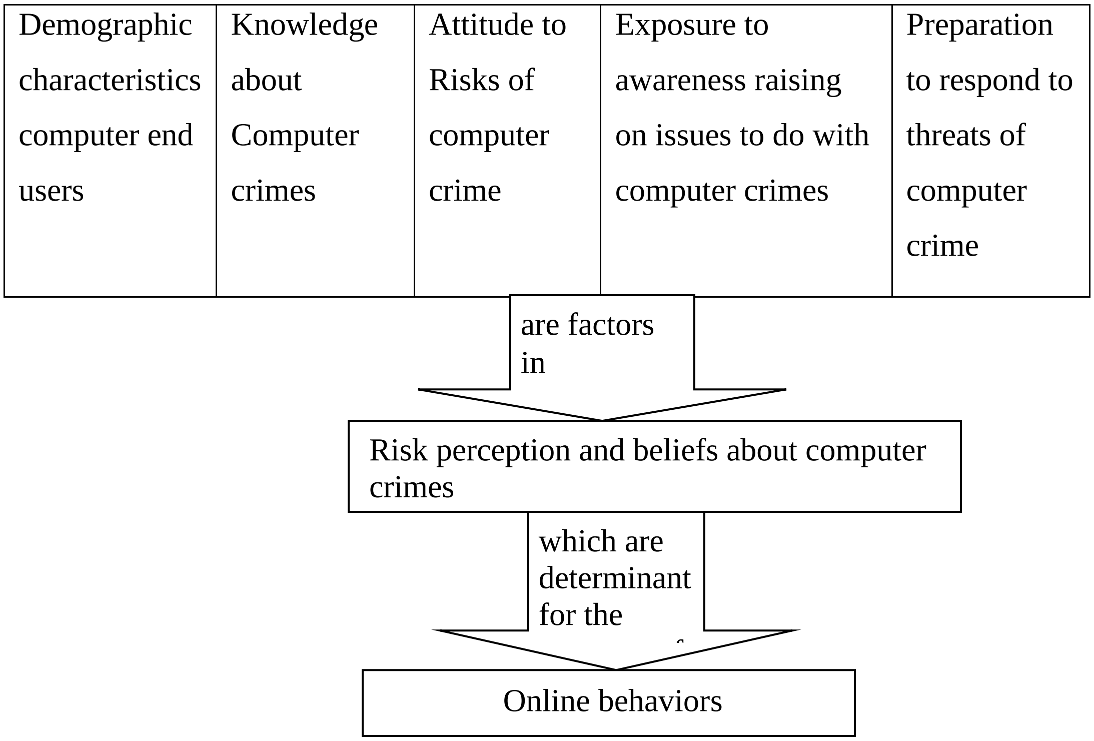
Demographic characteristics computer end users
Knowledge about Computer crimes
Attitude to Risks of computer crime
Exposure to awareness raising on issues to do with computer crimes
Preparation to respond to threats of computer crime
are factors in
Risk perception and beliefs about computer crimes
which are determinant for the
Online behaviors

Figure 2: A framework adapted from generic framework developed by Enders (2001)

Each of the factors mentioned above, which is a variable of interest in this research was ascertained by as section of the research tool that was developed. Looking at each of these variables in a little more details certain thing comes out.

- Demographic characteristics: these included the age of individual, gender and education level. This was necessary to determine whether the sample taken for the study can actually be generalized for the target population. Since these characteristics cannot be manipulated, demographic characteristic in a research is considered to be an independent variable.
- Knowledge about Computer crimes: This generally included the various types of cyber crimes that the user is aware. The measure here may include both the technological measures as well as hardware. To assess this we need to have a sliding scale where a user is totally unaware about

the existence of computer crimes to being fully aware about their existence. There is a possibility that a two – way relationship can exist between cyber crime knowledge and the attitude of the risks of the computer crime.

- Attitude to Risks of computer crime: This will include how the user perceive cyber crime threats and risks, in most cases this will include the scientific assessment of the accompanying risk of computer crime, and what the user perceive this scientific assessment. It will also include whether the user considers the risk as being harmless or not.
- Exposure to awareness raising on issues to do with computer crimes: This includes factors involved in whether the individual personally, or someone they know, has been exposed to awareness raising efforts about computer crimes. Under this factor there is need to look at whether the computer user has been exposed to any form of computer crime awareness training at all and if he has how effective it was. At the same time it will look at how the user has obtained the information he has about computer crimes. The aim is to look at the users experience with cyber crime awareness raising.
- Prepared to respond to threats of computer crime: This concept looks at perceived or actual ability to behave appropriately in cyber crimes risk situation; measure put in place by the end user to mitigate against these crimes. It includes such factors as access to necessary resources, feeling of responsibility and vulnerability when online.

2.10 Conceptual Model

According to Lewis (2013) awareness about cyber threats and readiness to counteract them not only does it have the potential to reduce the cost of cyber security but it also has the ability to reduce by over a half the number of successive attacks. In developing the conceptual model the assumption made is that both awareness and preparedness to deal with cyber threats has an effect on online behavior which in turn determines the frequency of cyber incidences an individual experiences**.** The aim of this framework is to clarify the range of factors that need to be considered in order to appropriately conceptualize the issues relating to awareness and preparedness.

From the framework developed by Enders (2001), the independent variables are: knowledge about Computer crimes; Attitude to risks of computer crime; preparation to respond to threats of computer crime

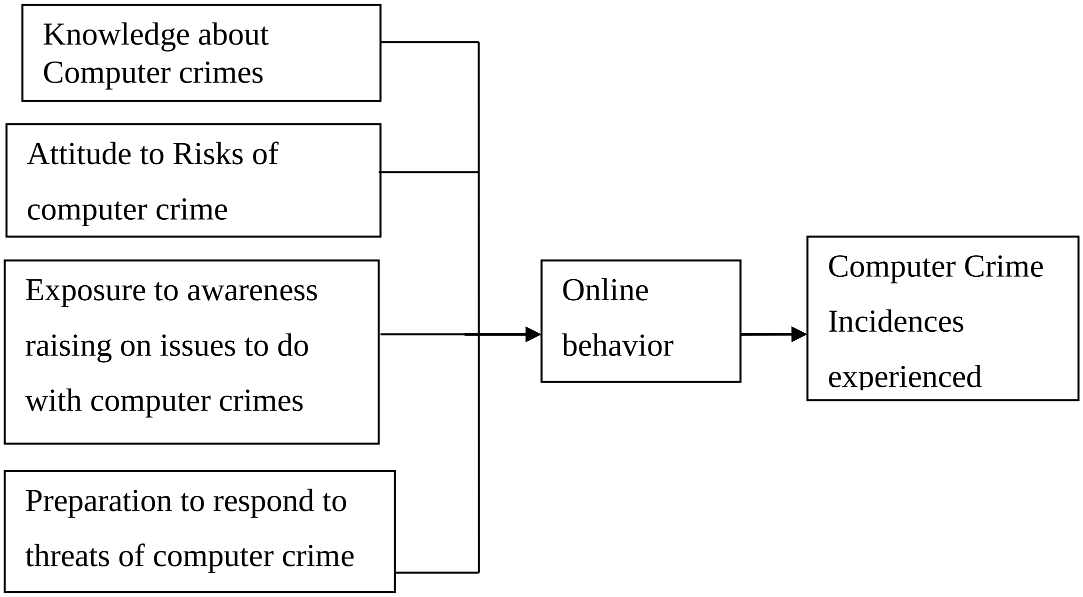
Knowledge about Computer crimes
Attitude to Risks of computer crime
Exposure to awareness raising on issues to do with computer crimes
Preparation to respond to threats of computer crime
Online behavior
Computer Crime Incidences experienced

Figure 3: Conceptual model

CHAPTER 3: RESEARCH METHODOLOGY

3.0 Introduction

This chapter deals with all the aspects involved in data collection that the researcher uses as the basis for his research findings, drawing of conclusions and also the basis of giving recommendations at the end of the study.

In general, this chapter on research methodology includes: the research design, the target population, the sample and the sampling technique, the instruments that will be used for collecting the data, the validity of the research instruments and the reliability of the research instruments for collecting the data, the data collection procedure and the data analysis technique that the researcher uses.

3.1 Research Design

In carrying out this research a descriptive survey design was used in assessing the awareness level and the state of preparedness of the internet end user in dealing with risks of computer crimes; since it was considered the most appropriate. This is given the fact that the researcher had no intention of influencing the various variables in this research. According to Mugenda and Mugenda (2003) a descriptive research determines and reports the way things are. The researcher does not in any way influence the various variables. Descriptive research is considered suitable in this particular case since as Kumar and Ranjit (2005) puts it "descriptive research attempts to describe systematically a situation, a problem, a phenomenon, service or a program or provide information about, say, a living condition of a community, or describe attitudes about an issue". Descriptive research have the ability to give room for probing for more information, exploring new ideas and simultaneously generating discussions and information on emerging concerns on the line of thought. A descriptive study describes the existing conditions and attitudes through observation and interpretation, and this is what this study intended to do.

3.2 Study Area, Target Population and Sampling Size

The target population for a survey is the entire set of units for which the survey data are to be used to make inferences (Lavraskas, 2008). The target population for this research is internet users in the country; but the research was carried out within Nairobi. The choice of Nairobi as area of carrying out the research, was informed by the fact that it was within easy reach of the researcher, thus cutting down on issue of cost and time; which are a constrain during research; as Mugenda and Mugenda (2003) affirms "research is a very expensive undertaking in terms of time and resources". As such it is necessary to cut down on cost of carrying out the research without compromising on the quality of the research work done.

The data collection was done in randomly selected cyber cafés within Nairobi County, with a total of twenty two cyber cafés being used, with majority of these cafés being within the central business district (CBD).

The main reason why cyber cafés were selected for the survey is that the people going there are being assumed to be computer literate. At the same time these people are assumed to be coming from different social backgrounds as well as having different levels of education. For these reasons they were taken to be a representative of a general computer/internet end user within the Nairobi County. According to CCK quarterly sector statistical report of 2012/2013 the estimated number of internet user in Kenya was given as 16.4 million people. The same report also acknowledges that there is no scientific method of estimating the number of internet users. This posed a challenge on how to estimate the number of internet users within Nairobi. To overcome this challenge; the population of the Nairobi County was considered as a ratio of the country's population and we approximated that this ratio is roughly the same ratio of internet users within the County.

The population of Nairobi around this time was estimated to be 3.4 million people while that of the country was estimated to be 40 million people (Kenya demographic profile, 2013). From these figures our target population of internet users within Nairobi is approximately $\frac{3.4}{40}$ x 16.4 million people. This gives a target population of approximately 1.4 million internet users. The number of internet user within the Nairobi is bound to be far much higher than this; given the fact that this being the capital city we expect it to have more internet users than any other urban centre. The estimated number of internet users within the County thus justifies the use of sampling as the method of data collection.

From the target population a sample is to be taken for the purpose of the study. Several ways are available for estimating the sample size. In this study we calculated the sample based on a simplified formula provided by Yamane (1967: 886); and quoted by several authors in recent past.

The formula is $n = \frac{N}{1+Ne^2}$ where n is the sample size, N is size of target population and e is the level of precision. The reason for doing this is to ensure the reliability of the results, which is achieved by obtaining the optimum sample size which is guaranteed by this formula. Obtaining a sample by this method ensures that it fulfills the requirements of efficiency, representativeness, reliability and flexibility. In this study we adopted a level of precision of ± 7%. Thus from a population of 1.4 million internet user $n = \frac{1.4 \text{ x } 10^6}{1+1.4 \text{ x } 10^6 \text{x} 0.07^2}$ = 204 respondents.

According to Israel (2009) "many researchers commonly add 10% to the sample size to compensate for persons that the researcher is unable to contact and at the same time they increased the sample size by 30% to compensate for nonresponsive respondent." Thus to compensate for those internet users who cannot be reached and also those who will get the questionnaires but they will not respond a total of 290 questionnaires were used to collect that data.

3.3 Research Strategy

The starting point of this research was a critical review of the existing literature on computer/cyber crimes and cyber security. Books, academic papers, journals and the internet were very significant data source in this preliminary study. After the literature review, a questionnaire was designed from information gathered from the literature. Thereafter survey using a self administered questionnaire was carried out to collect the primary data from the internet end users from randomly selected cyber cafés. The questionnaire resulted in quantitative data being collected from the sample population. The result from the research are supposed to be a true reflection of the target population, thus care was taken when doing the sampling to ensure validity and reliability of the data collected. To minimize bias during data collection multi – stage random sampling was done on the target population. This involved first selecting a cyber café at random then selecting the respondent randomly from the selected cyber.

According to Mugenda and Mugenda (2003) quantitative research is easier to analyze; thus the reason for using quantitative method of data collection. The data collected was analyzed using SPSS version 20.0 and Excel.

3.4 Research Questions

Since the intended research was going to be descriptive in nature, the questions for the research instrument were derived from the available literature on computer crimes. The questions provided the basis of the research to determine the awareness level as well as the level of preparedness in combating computer crimes among computer users. The questions were also be used to give an indication of how the internet users behave online.

3. 5 Data Collection Procedures

For the purpose of data collection multi – stage sampling was done. This involved randomly selecting the cyber cafés within Nairobi followed by randomly selecting the internet end user from the selected cyber cafés. The researcher sought permission to carry out the study in the selected cyber cafés from their management. This was done through a visit to the concerned cyber cafés and having a discussion with the management with an aim of getting their consent to carry out the research within the cyber cafés. After the consent was obtained, questionnaires were then administered to the users of cyber cafés who were also selected randomly. Those selected were first requested to answer the questionnaire and in the process the purpose of the research was explained to them; if they agreed to be respondents, the questionnaire was given to them. Those who were not willing to take part in the research were left out. The exercise which was initially expected to take two weeks took a total of three weeks; since some of the cyber cafés randomly selected were not willing to have the research undertaken in their premises. At the same time some of the respondents took a bit of time in answering the questionnaire as they wanted to engage the researcher in discussion rather than answering the questionnaire on their own.

To get a fair representation of the target population the number of questionnaires were restricted to between ten and fifteen per cyber café. The questionnaire itself had four sections. Section A was dealing with the demographic information about the respondent, section B had nine questions to gather some addition background information about the respondent. Section C had a total of twenty eight questions which were used to capture information on knowledge of computer crimes (KCC), attitude to risks of computer crimes (ACC), exposure to awareness raising (EAR), preparation to respond to computer crimes (PR) and online behavior (OB). In this section each item was measured on five point Likert – type scale which was aimed at testing the level agreement with the various indicators used. The scale had two extreme end points of "strongly agree" (5) to "strongly disagree" (1). Section D with two question captured information on computer incidences experienced by the internet user.

3. 6 Data Analysis Techniques

Data coding was done in order to ease the derivation summaries and meaning from it. The data collected was analyzed using Statistical Package for Social Scientist (SPSS) software version 20.0 and Excel. The data was presented using descriptive statistics in terms of frequencies, means and percentages. Descriptive statistics generally provide a powerful summary that can allow for comparison and conclusions to be drawn. The analysis of the questionnaire was done by tabulation using simple descriptive statistical measures such as frequency tables, means and percentages and then relevant implication of these values were noted; for conclusions to be able to be drawn. The purpose of using frequency tables, means and percentages was to make the work of drawing conclusions and passing the same to interested parties easier.

To evaluate the realization of our third objective a linear regression model was done. This was to assist in determining the level of contribution of awareness and preparedness to the overall online behavior of the internet users.

3.7 Mapping the Research Objectives on to Methodology

No.	Research Objective	How the objective were Achieved
1.	To assess the level of awareness on the existence of computer crimes among individual internet end users in Nairobi, Kenya.	By carrying out literature review in area of cyber crime then developing a questionnaire to be administered to the respondent.
2.	To assess the level of preparedness in dealing with computer crimes in Nairobi, Kenya by the individual internet end users.	Through a structured self-administered questionnaire to internet users in 20 cyber cafés to assess whether they consider security as an issue when going online
3.	To assess whether the level of awareness of computer crimes and level of preparedness in dealing with risks of computer crimes affect individual internet end users online behave.	By use of a linear model developed from the responses given through the self administered questionnaire.

Table 1: Mapping the research Objectives on to Methodology

3.8 Hypothesis

For purposes of testing the conceptual model the following hypothesis are proposed.

H_1: There is significant relationship between Knowledge of Computer Crimes and internet user On Line Behavior.

H_0: There is no significant relationship between Knowledge of Computer Crimes and internet user On Line Behavior.

H_2: There is a significant relationship between Attitudes to Risks of Computer Crime and Internet users On Line Behavior.

H_0: There is a no significant relationship between Attitudes to Risks of Computer Crime and Internet users On Line Behavior.

H_3: Exposure to awareness raising on issues to do with Computer Crimes has a significant relationship with internet users On Line Behavior.

H_0: Exposure to awareness raising on issues to do with Computer Crimes has no significant relationship with internet users On Line Behavior.

H_4: There is a significant relationship between Preparedness to deal with threats of Computer Crimes and Internet users On Line Behavior.

H_0: There is no significant relationship between Preparedness to deal with threats of Computer Crimes and Internet users On Line Behavior.

H5: Online Behavior has significant relationship with the number of Computer Crimes incidences experienced by an Internet user.

H_0: Online Behavior has no relationship with the number of Computer Crimes incidences experienced by an Internet user.

CHAPTER FOUR: ANALYSIS OF RESULTS AND INTERPRETATION.

4.0 Introduction

This chapter focuses on research results analysis and interpretation. The analysis focused on finding solutions to the research questions. The main research tool used in coming up with the research findings was self-administered questionnaire. After collecting the questionnaires from the internet users, coding was done, and then all incomplete questionnaires were removed. A total of 219 questionnaires remained out of the 290 that were used for data collection; this represented 76% of the total. This signifies that 24% of those surveyed are likely not to be having any idea what computer crime is.

4.1 Reliability and Validity of the Research Instrument

The research tool used was a structured questionnaire which was preferred as it provided a relatively simple and straightforward approach to the study; but at the same time the results obtained from it must be reliable and valid.

4.1.1 Reliability

“Reliability is an assessment of the internal consistency of the measurement instrument and a measure of the degree of homogeneity among the measurement items in a given construct” (Wamuyu & Maharaj, 2011). It is the assessment of whether the results remain consistent over repeated testing. According to Bhattacherjee (2012) reliability is the degree to which the measure of a construct is consistent or dependable. Thus reliability is a measure of the degree to which a research instrument yields consistent results or data after repeated trails; that is the instrument would give similar results in different situations or under similar circumstances but at a different time. To ensure reliability of the questionnaire it was pre – tested in two cyber cafés within Nairobi County; ten internet users being used for this activity. The aim was to check if the questionnaire will be clear and well understood by the respondents. During pre - testing certain issues especially to do with the language and the layout of the questionnaire were identified and rectified. To uphold the ethics of research the cyber café that were used during pre – testing of the research instrument we’re not included in the actual study.

Section	No. of Questions	Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items
Knowledge about Computer Crimes (KCC)	6	0.365	0.413
Attitude to risks of Computer Crime (ACC)	5	0.492	0.482
Exposure to Awareness Raising (EAR)	6	0.366	0.413
Preparation to Respond (PR)	6	0.611	0.632
Online Behavior (OB)	5	0.263	0.291

Table 2: Reliability table before elimination

On further analysis of the correlation between the various items, it was observed that the reliability could be improved by eliminating some of the questions in the various construct. In Knowledge about computer crimes two questions were omitted from any further analysis that is KCC3 and KCC4. In Attitude to risks of Computer Crimes one question was omitted; ACC4. In Exposure to awareness raising EAR1 and EAR4 were omitted, while in Online behavior OB4 and OB5 were omitted.

After the elimination of these questions the following table of reliability was obtained

Section	No. of Questions	Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items
Knowledge about Computer Crimes (KCC)	4	0.566	0.575
Attitude to risks of Computer Crime (ACC)	4	0.656	0.661
Exposure to Awareness Raising (EAR)	4	0.519	0.534
Preparation to Respond (PR)	6	0.611	0.632
Online Behavior (OB)	3	0.365	0.365

Table 3: Reliability table after elimination of some question

Even though most researchers urge that a value of 0.7 and above is the acceptable level of acceptability of Cronbach Alpha; according to Schmitt (1996) "there is no sacred level of acceptability or unacceptability of alpha". Following this argument then the values of Alpha's obtained above were used for the significance of internal consistency within the various constructs. The low values of Cronbach Alpha signify that the constructs being used for all the items lacks internal consistency.

4.1.2 Validity

Validity is the accuracy and meaningfulness of the inferences, which are based on the research results (Mugenda & Mugenda, 2003).There are two types validity, external and internal validity. According to Thorndike and Hagen quoted by Kothari (2004) "external validity is the degree to which research findings can be generalized to a population, settings, treatment variables and measurement variables". On the other hand "internal validity is the degree to which extraneous variables have been controlled for in the study" (Mugenda & Mugenda, 2003). To ensure internal validity, the survey questionnaire was pre-tested with 10 computer end users for meaning and semantics and then reviewed by an experts and experienced researcher. In order to measure the respondent opinion on various aspect computer crime awareness and preparedness each of the construct was measured using several statements.

4.2 Demographic Profile of the respondent

The tables below shows demographic characteristics of the respondents obtained from the questionnaire. Respondents were internet end users from randomly selected cyber cafés within Nairobi County.

4.2.1 Gender of internet user

	Number	Percent %	Valid Percent (%)	Cumulative Percent
Male	106	48.4	48.4	48.4
Female	113	51.6	51.6	100.0
Total	219	100.0	100.0	

Table 4: Gender of internet end user

From the table it is clear that there were more female cyber café user at 51.6% as compared to men at 48.4%.

4.2.2 Level of education of internet user

The table below gives us an idea of the distribution of level of education of the internet user.

Level	Number	Percent %	Valid Percent (%)	Cumulative Percent (%)
Postgraduate	40	18.3	18.3	18.3
Bachelor's Degree	93	42.5	42.5	60.7
Diploma	60	27.4	27.4	88.1
Others	26	11.9	11.9	100.0

Total	219	100.0	100.0	

Table 5: Level of education of internet users

From the table it is clear that the majority of internet users have a college level of education. Majority of the people frequenting cyber cafés in Nairobi County are educated and as such it is expected that their knowledge of computer crimes is high and they are aware of the essential basic safe guards that they needs to take when going on line.

The bar chart below represents both the percent and the frequency of level of education of internet users.

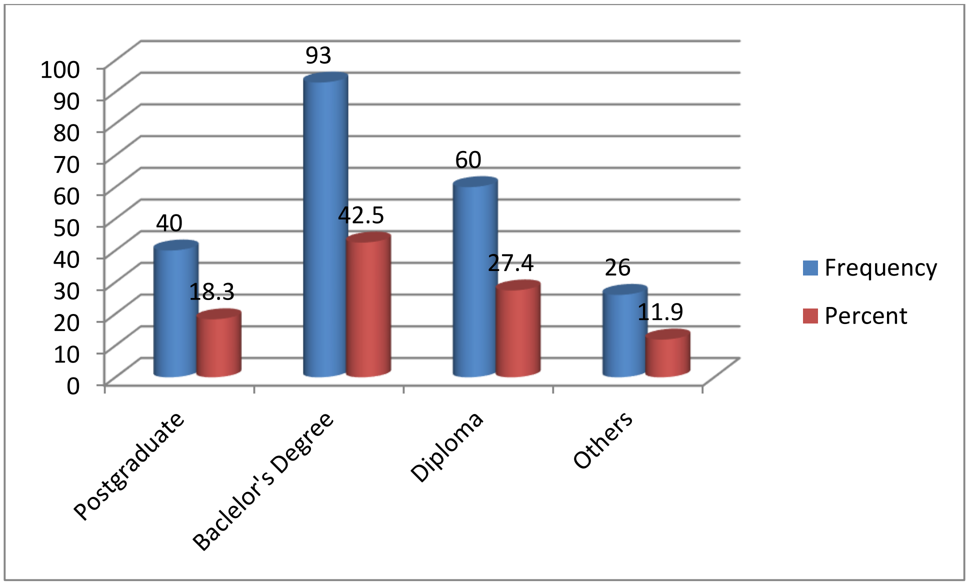

Figure 4: Level of education of internet user

4.2.3 Age of internet user

The below gives the age of the various users that undertook the study.

Age in Years	Number	Percent %	Valid Percent (%)	Cumulative Percent (%)
18-22 yrs	56	25.6	25.6	25.6
23-27 yrs	80	36.5	36.5	62.1
28-32 yrs	38	17.4	17.4	79.5
33-37 yrs	23	10.5	10.5	90.0
Above 38yrs	22	10.0	10.0	100.0
Total	219	100.0	100.0	

Table 6: Age of respondents

It is clear that the majority of the people using the cyber cafés were young people below the age of thirty years. They account for over 62.1% of the people visiting the cyber cafés.

4.3 Activities normally carried out online by the user

In this section we wanted to establish which kind of activities most of the respondents carry out online. The responses were to be selected from a given list. The purpose of these was to check whether the activities carried out places the users at higher risk than others.

Activity carried out online	Number of Respondents	Percent
Auction	6	2.7%
Gambling	9	4.1%
Shopping	32	14.6%
Banking	37	16.9%
Downloading music & movies	74	33.8%
Research	128	58.4%
Search for information	132	60.3%
Socializing	162	74%
Checking and replying Emails	174	79.5%

Table 7: Activities carried out online by the internet users

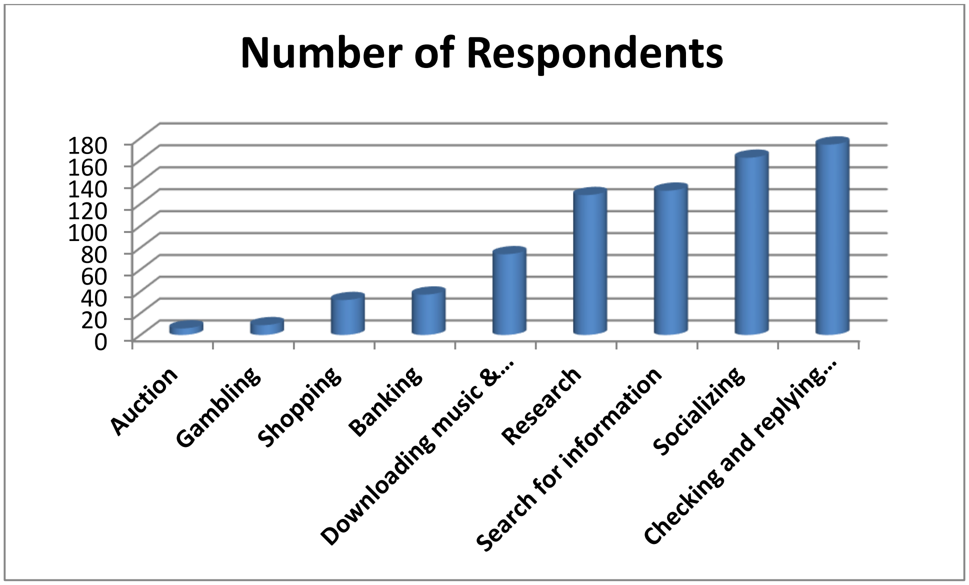

Figure 5: Activities normally carried out online by internet users

These activities carried out by the majority of the people might be considered low risk activities. This is considering that the information being shared or the activities being carried out is of very low risk. Activities like banking, auction, shopping and gambling attracts very few internet users. These activities can be considered to be high risks activities.

4.4 Awareness of existence of computer crime and knowledge of the same.

For the purposes of analysis in this particular section all those who strongly agreed and agreed were combined while those who strongly disagree were combined to those who disagreed. To a find out whether the internet end users have any knowledge about existence of computer crimes, two questions indifferent section of the questionnaire were posed to them, the first one in section B of the questionnaire wanted to find out whether as an internet user he/she is aware about the existence of computer crimes. The second question was posed in section C and it required the respondent to rate himself/herself on Likert like scale of 1 to 5 on the agreement with the statement that "there are risks involved when I am working on line." On getting the descriptive statistics of the two questions it show that very few people acknowledges that there are risks when one is working online. At the same time very high number of the purport to be aware about computer crimes. This can only mean that despite being aware about the existence of computer crime the person is totally detached from the effects of cyber crime. That is he does not consider himself to be at a risk.

The two tables below and the charts give a clear picture.

Responses	Frequency	Percent	Valid Percent	Cumulative Percent
Yes	194	88.6	88.6	88.6
No	25	11.4	11.4	100.0
Total	219	100.0	100.0	

Table 8: Internet end users aware of the existence of computer crimes

From our statistics 88.6% acknowledges that computer crimes are there while 11.4% are not aware

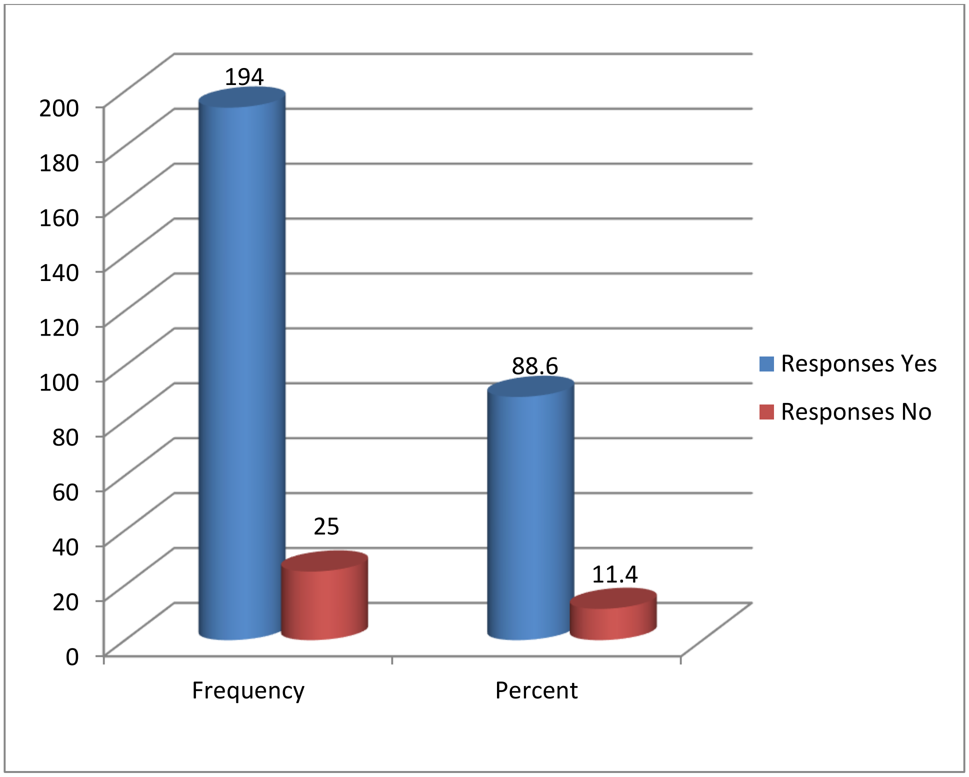

Figure 6: Chart of internet users who are aware of the existence of computer crime

Responses	Frequency	Percent	Valid Percent	Cumulative Percent
Agree	179	81.7	81.7	81.7
Neutral	26	11.9	11.9	93.6
Disagree	14	6.4	6.4	100.0
Total	219	100.0	100.0	

Table 9: There are risks involved when working online.

From the table it is clear that 81.7% of the respondents do agree that there are risks while working online.

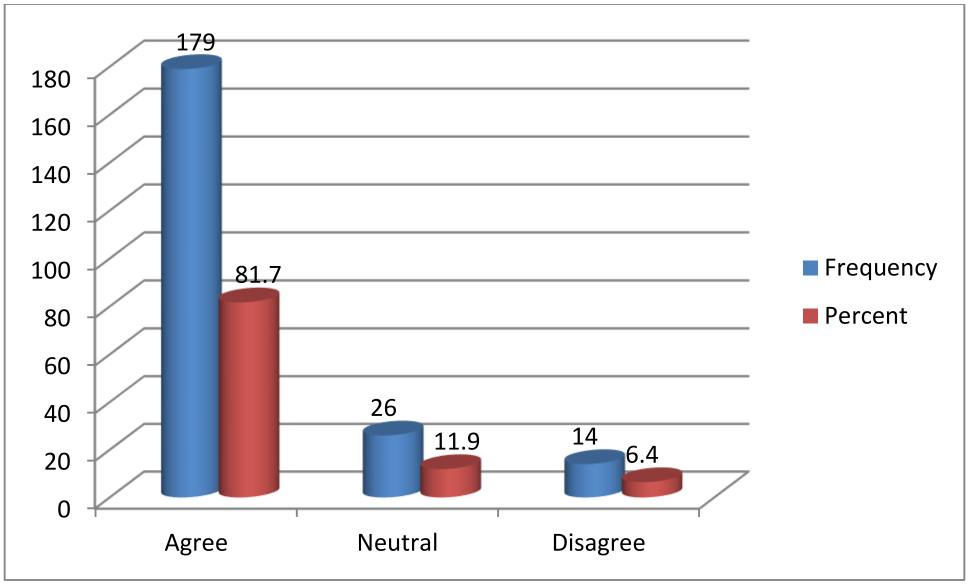

Figure 7: Acknowledgement that there are risks when one is online

It is clear that even though the two questions are basically asking for the same thing but in different sections of the questionnaire there is difference between those who answers the question in the affirmative. In one question 88.6% of respondents acknowledge that computer crimes do exists while in the other question only 81.7% acknowledges that they are at risk when going on line. This shows a variance of 6.9% of the respondents this is indicative about the knowledge levels about computer crimes in that as much as majority are indicating that they are aware about computer crimes this might not be the case on the ground.

4.5 Awareness level of internet end users

To assess the awareness level of the internet user a new variable Awareness (A) was computed from the remaining constructs of Knowledge of computer crime (KCC), Attitude to risks of computer crimes (ACC) and Exposure to awareness raising (EAR). This new variable was given scale of 0 to 10

Where A = (((KCC1 + KCC2 + KCC5 + KCC6 + ACC1 + ACC2 + ACC3 + ACC5 + EAR2 + EAR3 + EAR5 + EAR6) -12) /48) *10.

On analyzing the descriptive statistics of Awareness we note that the number of internet user among the general public, on a scale of zero (0) to ten (10), who can be rated as being aware about computer crimes is very high. Those with a value of zero are considered to be having no knowledge at all while those with a value of ten are the most knowledgeable about computer crimes.

Scale	Frequency	Percent	Valid Percent	Cumulative Percent
2.7083	2	0.9	0.9	0.9
3.3333	1	0.5	0.5	1.4
3.7500	1	0.5	0.5	1.8
3.9583	1	0.5	0.5	2.3
4.3750	6	2.7	2.7	5.0
4.5833	3	1.4	1.4	6.4
4.7917	12	5.5	5.5	11.9
5.0000	7	3.2	3.2	15.1
5.2083	9	4.1	4.1	19.2
5.4167	18	8.2	8.2	27.4
5.6250	14	6.4	6.4	33.8
5.8333	23	10.5	10.5	44.3
6.0417	25	11.4	11.4	55.7
6.2500	34	15.5	15.5	71.2
6.4583	11	5.0	5.0	76.3
6.6667	16	7.3	7.3	83.6
6.8750	10	4.6	4.6	88.1
7.0833	7	3.2	3.2	91.3
7.2917	11	5.0	5.0	96.3
7.5000	1	0.5	0.5	96.8
7.7083	1	0.5	0.5	97.3
7.9167	3	1.4	1.4	98.6
8.1250	2	0.9	0.9	99.5
8.5417	1	0.5	0.5	100.0
Total	219	100.0	100.0	

Table 10: Descriptive statistics for Awareness about computer crimes

From the table it is clear that among those sampled over 84.9% of the respondent have a value of awareness above 5 on the scale of 0 to 10.

The histogram and the normal curve in figure 2 shows the distribution of level awareness among the internet user.

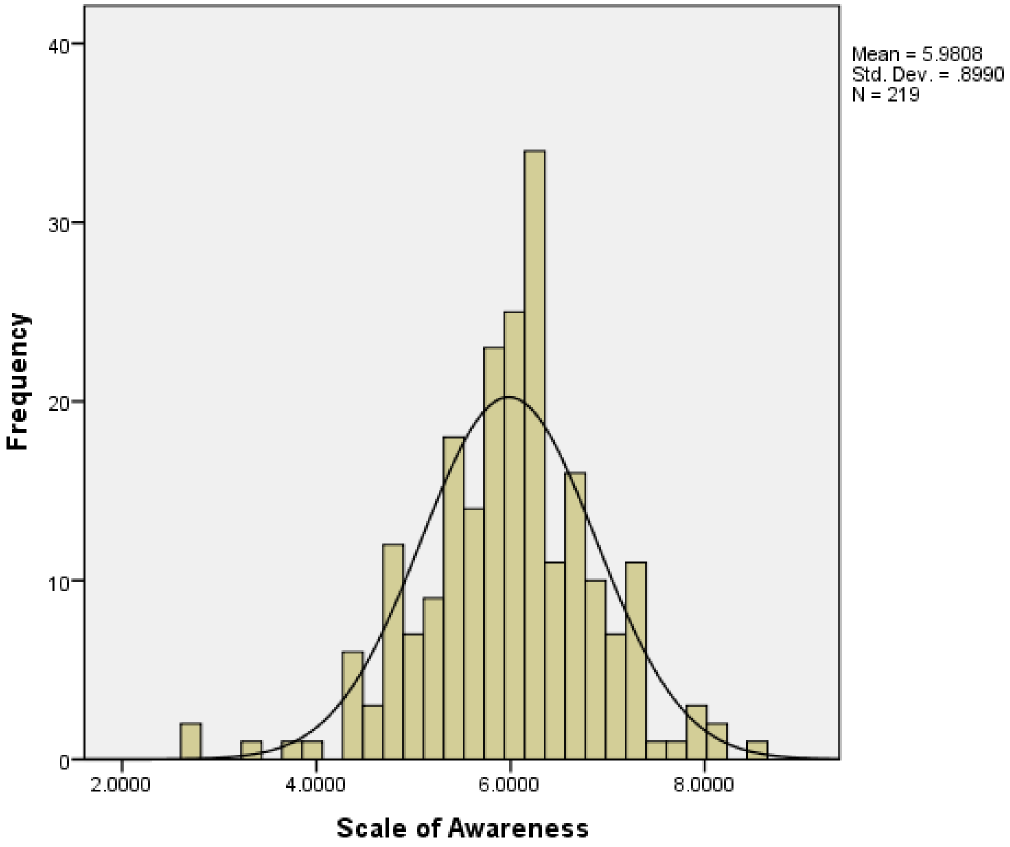

Figure 8: Scale of Awareness

It clear that the mean value of the awareness level for those interviewed is about 6 on the scale of 0 to 10. This signifies high level of awareness about computer crimes among those surveyed.

4.6 Level of preparedness of internet end users to deal with threats of computer crimes

To determine the level of preparedness of the internet users a new variable Preparedness (P) was computed from all the constructs of Preparation to respond to threats of computer crimes (PR). Where P = (((PR1+ PR2 +PR3+ PR4+ PR5 +

PR6)-6)/24)*10. This variable also had a scale of zero to ten. With a value of zero indicating total lack of any form of preparedness while a value of ten indicating very high degree of preparedness. From descriptive statistical analysis of the Preparedness it can also be seen that the highest percent of internet users are prepared to deal with threats of computer crimes.

Scale	Frequency	Percent	Valid Percent	Cumulative Percent
3.3333	2	0.9	0.9	0.9
4.5833	2	0.9	0.9	1.8
5.0000	3	1.4	1.4	3.2
5.4167	3	1.4	1.4	4.6
5.8333	7	3.2	3.2	7.8
6.2500	10	4.6	4.6	12.3
6.6667	12	5.5	5.5	17.8
7.0833	20	9.1	9.1	26.9
7.5000	27	12.3	12.3	39.3
7.9167	29	13.2	13.2	52.5
8.3333	20	9.1	9.1	61.6
8.7500	21	9.6	9.6	71.2
9.1667	31	14.2	14.2	85.4
9.5833	14	6.4	6.4	91.8
10.0000	18	8.2	8.2	100.0
Total	219	100.0	100.0	

Table 11: Level of preparedness among internet end user

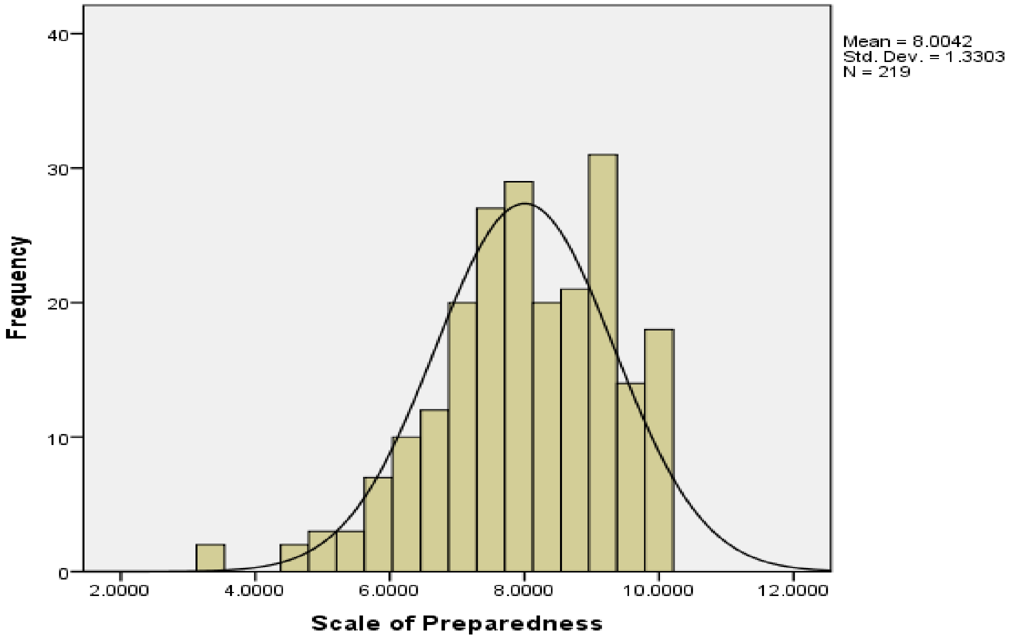

Figure 9: Scale of Preparedness

Using both the table of statistics and the histogram we can actually see that the level of preparedness among the internet users is very high. From graph it is clear that the minority of the internet users level of preparedness lies between 0 and 4. With a mean value of level of preparedness being at 8 it signifies that those interviewed are actually very much aware of what safe guards they need to be put in place for themselves to be considered safe.

4.7 Correlation between Online behavior and Awareness

The table below shows the correlation between awareness and online behavior

		Awareness	Online Behaviour
Awareness	Pearson Correlation	1	0.230**
	Sig. (2-tailed)		0.001
Online Behaviour	Pearson Correlation	0.230**	1
	Sig. (2-tailed)	0.001	

**. Correlation is significant at the 0.01 level (2-tailed).

Table 12: Correlation between Awareness and Online behavior

According to Mugenda and Mugenda (2003) the strength of the association between two variables is determined by the absolute value of the coefficient of correlation between the two in our case the magnitude of correlation between the two variables is very small. That at 0.230 and significance level of 0.001 it tell us that the relation between the two is very weak. But all the same it tells us that an increase in the Awareness index will also mean an increase in a positive online behavior.

4.8 Correlation between Online Behavior and Preparedness

The table below shows the correlation between online behavior and Preparedness.

		Online Behavior	Preparedness
Online Behavior	Pearson Correlation	1	0.228**
	Sig. (2-tailed)		0.001
Preparedness	Pearson Correlation	0.228**	1
	Sig. (2-tailed)	0.001	

**. Correlation is significant at the 0.01 level (2-tailed).

Table 13: Correlation between Preparedness and Online Behavior

At level of significance of 0.001 the relationship between the two variables is not very strong. All the same a positive value of this relationship signifies that an increase in the level of preparedness also signifies an increase in positive online behavior.

4.9 Computer crimes Incidences experienced in one Year.

The chart below shows the number of people who have experienced different types of computer crime incidences within one year. From the chart it is clear that the majority of the respondents have experienced cases of spam mails followed by virus or worms. The number of respondents also experiencing other forms of incidences also remains quite significant. This is despite the high level of awareness and preparedness which is being signified from the data collected. This can only mean that despite what the data is telling us the individual internet users are at very high risks. And at the same time the level of awareness and preparedness might be wanting.

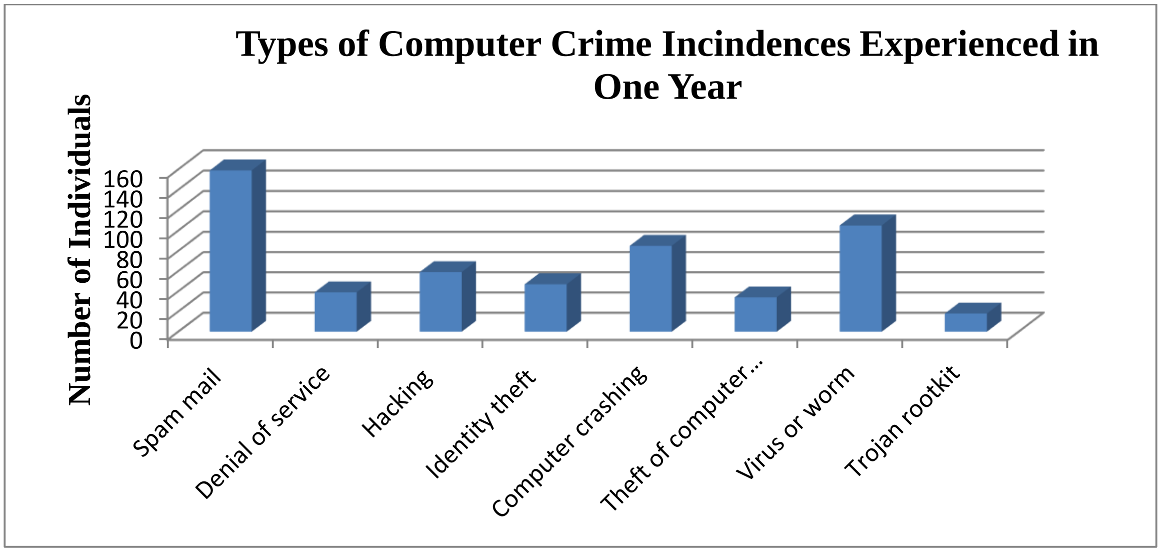

Figure 10: Types of computer crimes Incidences experienced in one Year

4.10 Number of Spam mail incidences experienced in one year.

Considering the spam mail incidences that are experienced by users within the year, we obtain the chart below.

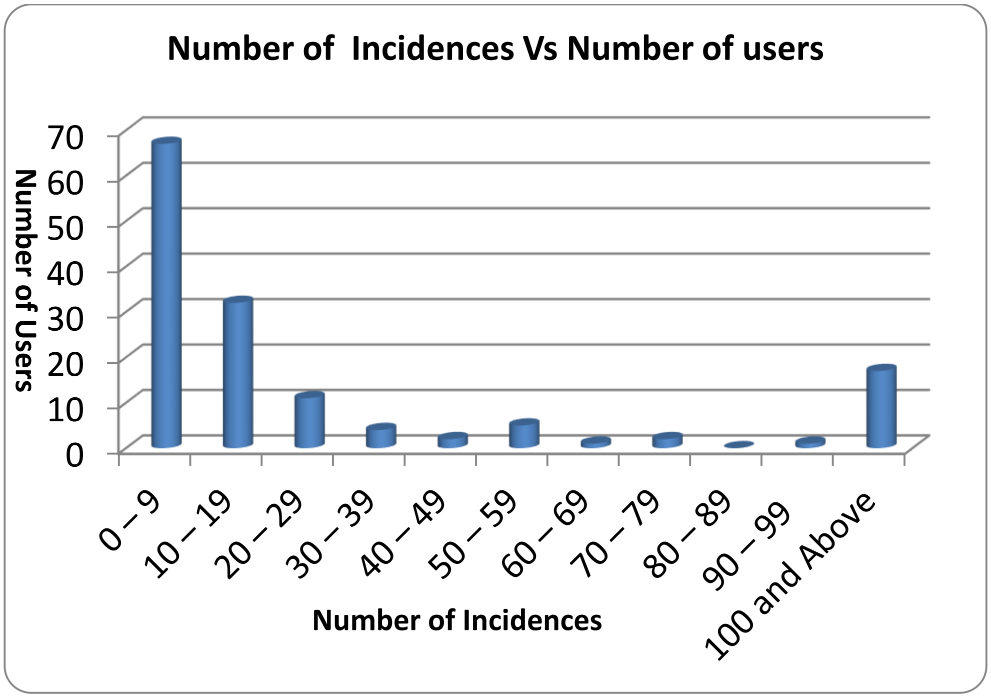

Figure 11: Number of Incidences vs number of Users

In our questionnaire we had requested that the user indicate the number of incidences he has experienced within the last one year and also indicated the number of times these incidences have been experienced. We note that after grouping the incidences the majority of the 142 respondents who had indicated that they had experienced spam mail had between 0 to 19 incidences. On the other extreme end we observe that the number of people reporting very high incidences of spam mail is also sizeable.

4.11 Hypothesis Validation

The table below gives the summary of Pearson Correlation between the independent variables and the level of On Line Behavior on our calculated scale. The table will be used in validation of the hypothesis.

Variables	Correlation Coefficient	Sig. (2 tailed)	Interpretation
KCC & B	0.028	0.677	Not Significant
ACC & B	0.075	0.268	Not Significant
EAR & B	0.144	0.033	Significant
A & B	0.230	0.001	Significant
P & B	0.228	0.001	Significant

Table 14: Summary of Pearson Correlation between the independent variables and calculated value of On Line Behavior

Considering the first hypothesis**, H_1**: there is significant relationship between **Knowledge of Computer Crimes** and internet user **On Line Behavior** and the corresponding null hypothesis **H_0**: there is no relationship between **Knowledge of Computer Crimes** and internet user **On Line Behavior**. On testing the null hypothesis we note from table 14 that the correlation coefficient between Knowledge about Computer Crimes and On Line Behavior is + 0.028. The correlation results of KCC and B indicates that the two variables have a very weak positive correlation. The significance (2 tailed) of this correlation is 0.677, this is far greater than 0.05, implying that this relationship is not significant. Thus we cannot reject the null hypothesis **H_0**. This is supported by the fact that the coefficient of correlation which is 0.028 is very small this is almost equal to zero. When the correlation between two variables is zero it signifies that there is no relation between them. Thus we can ignore the alternative hypothesis.

H_2: There is a significant relationship between **Attitudes to Risks of Computer Crime** and internet users **On Line Behavior**; the corresponding null hypothesis **H_0**: There is a no significant relationship between **Attitudes to Risks of Computer Crime** and internet users **On Line Behavior**. Considering the results from table 14, the coefficient of correlation of the two variables is 0.075 which shows a very weak positive correlation; the significance (2 tailed) is 0.268. This implies that the null hypothesis H_0 is not supported by any statistical evidence and as such we are unable to reject the hypothesis H_0. Thus we can conclude that there is no relationship between the **online behavior** and **attitude to risks of computer**

crimes, this is actually supported by the coefficient of correlation of 0.075 which is almost zero.

H_3: **Exposure to awareness raising** on issues to do with Computer Crimes has a significant relationship with internet users **On Line Behavior**; the corresponding null hypothesis is **H_0**: **Exposure to awareness raising** on issues to do with Computer Crimes has no significant relationship with internet users **On Line Behavior**. From table 14 the coefficient of correlation is 0.144, meaning a positive correlation while the significance of this relationship is 0.033, thus at 0.05 significance level this value is significant. Thus we reject our null hypothesis H_0. There is statistical evidence supporting that **Exposure to awareness rising** does have significant relationship with internet users **On Line Behavior**. Thus we are justified in accepting the alternative hypothesis H_3.

H_4: There is a significant relationship between **Preparedness** to deal with threats of Computer Crimes and Internet users **On Line Behavior**; the corresponding null hypothesis is **H_0**: There is no significant relationship between **Preparedness** to deal with threats of computer crimes and Internet users **On Line Behavior**. From table 14 we note that the correlations coefficient is 0.228 while the significance is 0.001 (2 tailed). Thus we reject the hypothesis H_0. This implies that we can accept our hypothesis H_4. The coefficient of correlation even though weak supports this observation.

H_5: **Online Behavior** has significant relationship with the number of **Computer Crimes incidences** experienced by an Internet user; the corresponding null hypothesis is **H_0**: **Online Behavior** has no relationship with the number of **Computer Crimes incidences** experienced by an Internet user. The computer crimes incidences experienced by different users in the course of the year were not the same. Thus to test this hypothesis we considered these incidences that were experienced by the majority of users. From figure 10 we considered spam mails and virus which appeared to be the most common the incidences experienced by the majority of internet users.

Variables	Correlation Coefficient	Sig. (2 tailed)	Interpretation
B & Spam Mails	-0.118	0.138	Not Significant
B & Virus / Worms	0.141	0.206	Not Significant

Table 15: Correlation between Online Behavior (B) and Computer Crime incidences (CCI)

From the table we note that Online Behavior and Spam mail incidences have a negative correlation. The scatter graph below shows the kind of relationship between Spam mail incidences and Online Behavior.

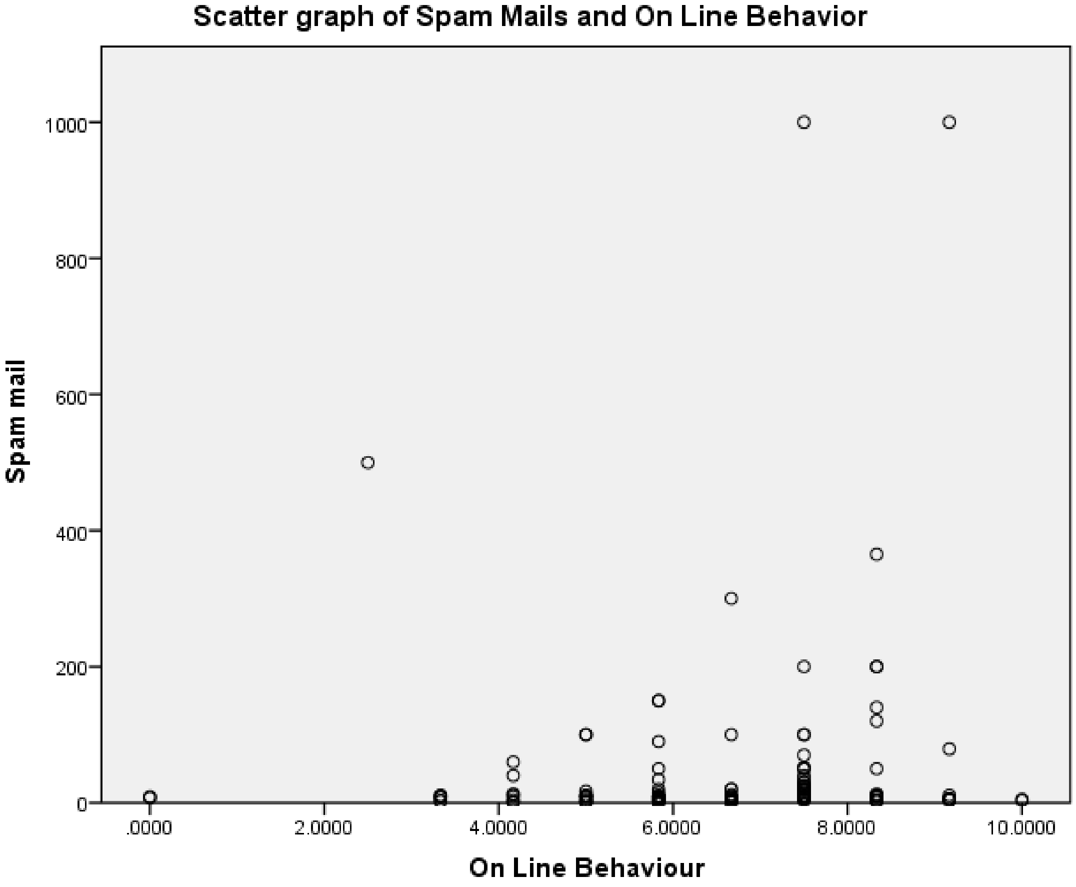

Figure 12: Scatter graph of Spam Mails and On Line Behavior

Comparing incidences of Virus and Online Behavior we note that the two has a positive correlation but this relation is a weak one, with a correlation coefficient of 0.141. But considering the two constructs (Spam mail and Virus) we note that at significance level of 0.05 (2 tailed) the two are not significant; this is given the fact that the values of the two are 0.138 and 0.206 respectively which is greater than 0.05. For that reason we cannot reject the null hypothesis H_0.

4.12 Linear Regression Model

Regression analysis is used when a researcher is interested in finding out whether an independent variable predicts a given dependent variable (Mugenda & Mugenda, 2003). In this case from the validation of the hypothesis we note that the Online Behavior (B) is dependent on both Awareness (A) and Preparedness (P). In order to find out the correlation between the user Online Behavior and the level of Awareness a new variable OnlineBehavior (B) was computed from the remaining constructs of OB after the others were eliminated after the Cronbach Alpha coefficient analysis was done on those construct. The new variable was given by On line Behavior **(B) = (((OB1+ OB2 + OB3) – 3)/12) *10.** This variable has a scale ranging from zero (0) to ten (10). With a zero indicating negative online behavior while a ten indicating a positive online behavior. Considering that there is a relationship between On line Behavior, Awareness (A) and Preparedness (P) even though weak; we presumed that then that this relation is a linear one and is governed by the equation $Y = a + b_1X_1 + b_2X_2$ as given by Kothari (2004), where Y is the dependent variable, X_1 and X_2 are the independent variables, ‘a’, ‘b_1’ and ‘b_2’ are the constants. In our case this equation translates to $B = a + b_1A + b_2P$. Using the values obtained for B, A and P and using SPSS version 20.0 for analysis we obtain the following information.

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics				
					R Square Change	F Change	df1	df2	Sig. F Change
1	0.293[a]	0.086	0.077	1.7235218	0.086	10.138	2	216	.000

a. Predictors: (Constant), Preparedness, Awareness

Table 16: Model Summary

Model	Unstandardized Coefficients		Standardized Coefficients	T	Sig.	95.0% Confidence Interval for B		Correlations		
	B	Std. Error	Beta			Lower Bound	Upper Bound	Zero-order	Partial	Part
(Constant)	2.200	0.955		2.303	0.022	0.317	4.082			
Awareness	0.377	0.133	.189	2.832	0.005	0.115	0.640	0.230	0.189	0.184
Preparedness	0.251	0.090	.186	2.785	0.006	0.073	0.428	0.228	0.186	0.181

Table 17: Coefficients of the model

From table 16 we note that the value of R^2, the coefficient of determination, is only 0.086. This means that the amount of variation in On line Behavior that can be explained by both Awareness and Preparedness is very minimal. This means that Awareness and Preparedness combined according to this model can only be able to account for only 8.6% of the variation in On Line Behavior of the internet end user. Thus the rest of 91.4% of the variation of Online Behavior cannot be explained by the variables in this model.

From table 17, we note that the constant ‘a’ is equal to 2.2; ‘b_1’ is equal to 0.377 while ‘b_2’ is equal to 0.251. Thus our model reduces to **B = 2.2 + 0.377A +0.251P**. This is in agreement with our hypothesis validation in that both Awareness and Preparedness have a correlation with the online behavior; even though it is a very weak one.

4.13 Summary of our Findings

The table below gives the summary of our research findings.

Hypothesis	**Dependent Variable**	**Independent Variable**	**Explanation**
H_1	B	KCC	KCC is Positively associated with B although it is a weak relation. The relationship is not Significant. Thus we fail to reject the hypothesis H_0
H_2	B	ACC	ACC is weakly but positively correlated to B. This relationship is not significant. Thus we cannot reject the hypothesis H_0.
H_3	B	EAR	EAR has a positive correlation with B. This correlation is significant. Thus we reject the hypothesis H_0
H_4	B	P	P and B are positively correlated and they are significant. Therefore we reject the hypothesis H_0.
H_5	Computer Crime Incidences	B	B and Computer Crime Incidences have weak correlation between them. At significance level of 0.05 this is not significant thus we cannot reject the hypothesis H_0.

Table 18: Summary of Findings

CHAPTER FIVE: DISCUSSIONS, CONCLUSIONS AND RECOMMENDATION

5.0 Discussion

From the statistical analysis we see that even though the level of Preparedness and Awareness are very high; certain things do not add up. Out of the 290 questionnaires given out 24% of them were not completed. This is a very high number if it is reflection of the actual population from which the sampling was done. The assumption being made here is that the likely reason why they never answered the questionnaire is that they had no ideal at all what computer crimes are. In section C of the questionnaire a Likert like scale was used to assess the internet user’s agreement with some given statements that were meant to assess their level of knowledge about computer crimes, their attitude to computer crimes, exposure to awareness raising on issues of computer crimes preparation and their actual online behavior. In all the constructs used to measure various variables in this section the number of people who were neutral was very high; indicating that this group of people can go either way. This might be an indicator that quite a number of the people who were sampled were giving the answer that they thought was expected in the survey; rather than what they believed in as far as computer crimes are concerned. Considering the knowledge and attitude about computer crimes which mostly dealt with the issue of the use of password; which is normally considered the most basic of security measures the number of the people who were neutral as far as safe use of the password and those who disagreed was relatively high. These shows that despite the perceived high level of awareness among those sampled the people are not very sure of what constitute computer crimes and the subsequent risks of the same.

This might be attributed to exposure to issues of computer crimes. The implication being that the users have very minimal exposure to computer crimes. At the same time it is possible that the majority of them have very rudiment knowledge of computer crimes. This low level of awareness thus explains the high number of computer crime incidences experienced by these users. The assumption being taken in this research is that once a user is aware about computer crimes then he is expected to be very keen when going on line such that his activities does not put him at risk.

On evaluating Awareness from KCC, ACC and EAR the three constructs can now be replaced by the new construct in our conceptual model. Having this in mind then our framework changes from;

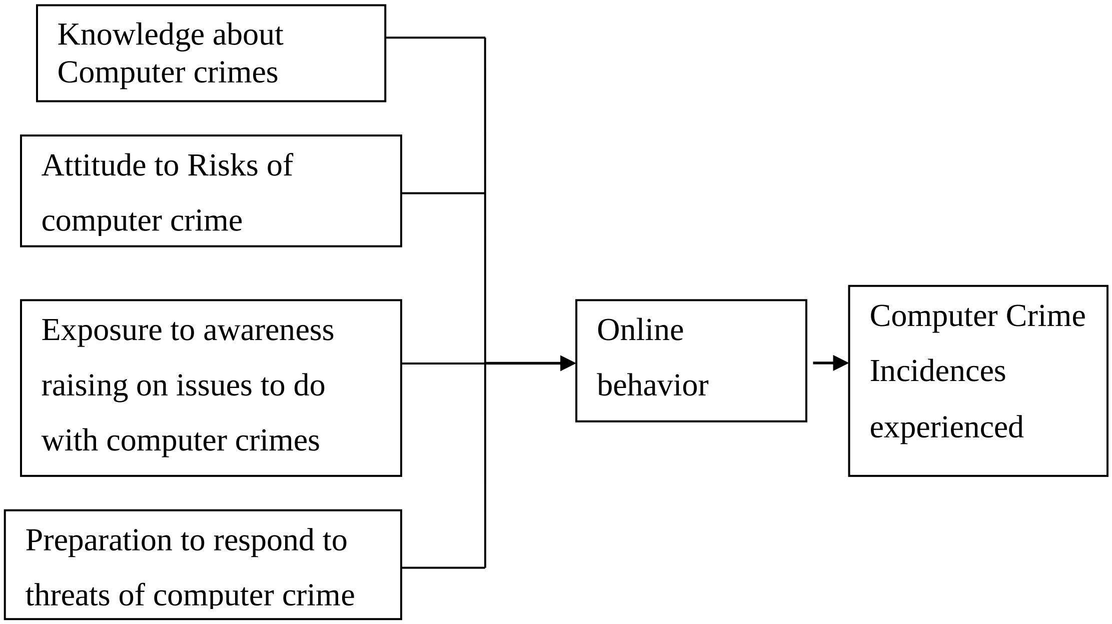
Knowledge about Computer crimes
Attitude to Risks of computer crime
Exposure to awareness raising on issues to do with computer crimes
Preparation to respond to threats of computer crime
Online behavior
Computer Crime Incidences experienced

Figure 13: Conceptual model

The refined and final framework is as shown below which is based on our research findings.

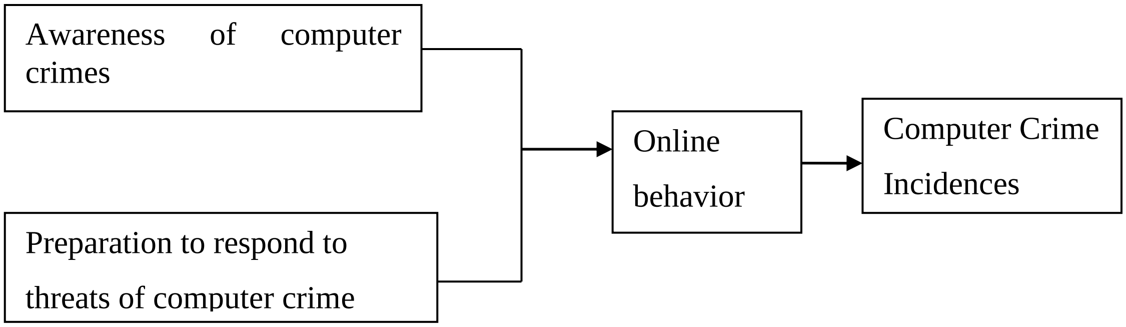
Awareness of computer crimes
Preparation to respond to threats of computer crime
Online behavior
Computer Crime Incidences

Figure 14: Final model

5.1 Conclusion

Considering the hypotheses that are being validated in this research we note that for **H_1**, where we are assuming that there is a significant relationship between Knowledge of computer crimes and the users Online Behavior; we note even though there is a correlation, it is a very weak one at 0.028. Considering level of significance which is at 95% we are unable to reject the corresponding null hypothesis. This weak correlation may be attributed to the lack of internal consistency in our constructs. This is given fact that the Cronbach alpha for all our various construct was below the acceptable level of 0.7. Thus we can't conclusively conclude that Knowledge of computer crime will influence the online behavior of internet users within the general public.

On the second hypothesis **H_2**, which was dealing with the attitude to risks of computer crimes among the internet users and their on line behavior; we note that the correlation is also very weak but the significance level is far above the 0.05 value. Thus we cannot reject the corresponding **H_0**. The implication is that the attitude of the user towards computer crimes has no direct implication on their online behavior. Given the challenge with the Cronbach Alpha we can't conclusively assume that there is no relationship between attitude and online behavior. This is based on our statistical analysis.

For **H_3**, exposure to awareness raising on issues to do with Computer Crimes has a significant relationship with internet users On Line Behavior. The corresponding null hypothesis is rejected on the ground that there is statistical evidence to show that there is positive correlation between the two. This implies that when a user is exposed to awareness raising issues his online is affected and as such we are likely to find the user behaving more cautiously when online unlike a user who has not been exposed to awareness raising. This is on matters to do with computer crimes.

H_4, there is significant relationship between Preparedness to deal with threats of Computer Crimes and Internet users On Line Behavior. We note that there is statistical evidence to allow us reject the corresponding null hypothesis. This implies that the kind of preparation that we have put in place will in most cases dictate how we behave when we go online. Therefore preparation to deal with threats of computer crimes affects the Online Behavior of the internet users.

H_5 that assumes that online behavior has a significant relationship with the number of computer crime incidences a user experiences. From table 15 we note that at significance level of 5% the two construct considered in this particular case are not significant. As a result of thus we cannot be able to reject the corresponding null hypothesis. This actually goes against the expectation in that, irresponsible online behavior is bound to expose one to very high risks of computer crime incidences. In terms of correlation we note that there is a correlation between computer crime incidences and online behavior but at the level of significance, this is not significant. It is therefore safe to assume that good Online Behavior is bound to reduce the number of computer crime incidences experienced by the internet users.

From the onset; this study was undertaken from the perspective that; in order be able to come up with informed policies that govern internet usage in the general public it is important to know the level of awareness and preparedness of the internet users. It was also assumed that awareness and preparedness has very big impact on how users behave online. The fact is; unlike organizations which have got rules and policies governing how individuals go online to access the organization information or use of organizations software and hard wares, the same rules are lacking when we come to the general public. Therefore basis of formulating policies and strategies to govern the internet usage within the general public is urgently needed. This way a country is able to safeguard the information held by the individuals privately as well as information held in public domain which is likely to be misused by unscrupulous individuals within the general public.

From our research it is clear that the level of Awareness and Preparedness have very little effect on the On Line Behavior of the internet end users. This can be deduced from the linear regression model which shows that both awareness and preparedness can only account for 8.6% of the variation in the online behavior of the internet users within the general public. Maybe this can be attributed to the fact that most of the activities being carried out by the group that was sampled can be considered to be low risks activities when one is online. This idea that the activities they are carrying out are low risks activities means that they are likely not to be very keen on security issues. This has the possibility of exposing them to cases of identity theft as well as other computer crimes.

When embarking on this study one of the limitations we noted was that the group within which the survey was to be under taken might not be within the cutting edge of ICT, and as such the information that they are likely to give might not be sufficient to make well informed decisions. This might explain the low variation of the online behavior with the perceived awareness and preparedness. The calculated value of awareness and preparedness appears to be quite high, but the percentage the account for the variation in the online behavior is extremely low. This is a total contrast from the expectation.

5.2 Recommendations

There is need to develop a strategy of how to increase the knowledge about computer crime within the general public. From our findings we note that knowledge of computer crime has some positive influence on how users behave on line. This bound to reduce the number of computer crime incidences originating from the general public. There are no set policies or rules on how one should behave when going online within the general public; this is unlike corporations which have the policies and rules that governs how their employees are expected to behave when online and within the corporation network; the same does not apply to the general public especially when going online when at home and other locations outside their offices.

The risks of exposure to computer crimes within the country will remain high as long as the knowledge of the same remains low within the general public. Chance of home computers being compromised and used as botnet thus becomes very high. To mitigate against this the knowledge about computer crimes needs to be raised within the general public thus the chances incidences of computer crime happening to the internet user will be reduced.

It is important that a positive attitude about risks of computer crime be cultivated within the general public. This attitude will have big impact on how individuals behave when going online and using personal computers at home. Thus it is important for ways and means to be explored on how to inculcate positive attitude towards risks of computer crimes within the general public. One way of doing this is increasing the awareness about computer crimes and sensitizing the internet users of the risk that are there when one is online.

Measures should put in place to ensure that the cost of enhancing the level of preparedness to handle the risks of computer crimes among the general public is at an affordable level; that is the cost of anti- virus and other softwares meant to enhance the levels of the preparedness should be made affordable. This way it will be easier for the members of general public to be able to prepare adequately to deal with threats of computer crimes. Educating the general public on how they should safeguard their information when going online should also be under taken regularly.

In future it would be important carry out group discussion with the internet end users in order to actually determine the extent of the level of awareness and preparedness about computer crimes; this is rather than relying only on self administered questionnaire to determine the level of awareness and preparedness. This way issues that are likely to be ambiguous are likely to be sorted out and clarified in the process of data collection.

Rather than doing multi – level random sampling it would be important to adopt or use purposeful sampling in order to gain proper representation of respondents in terms of age and level of education. This way all groups will be well represented when collecting data and as such it will be easier when generalizing the findings of this research to the general public.

5.3 Future Work

This research only focused on knowledge, attitude, exposure to issues to do with raising awareness and preparedness but it did not consider the factor like cost of having safeguards in place for one to be considered to be prepared. It would be important to consider in future the impact of cost on having the necessary safety measures in place on levels of preparedness. It would also be important to find out what efforts the internet end user needs to have put in place in order to be considered as being prepared. That is certain parameters should be considered to be in place in order for one to be considered prepared.

In future it would be important to study the effect of past experience of computer crime incidences on the On Line Behavior of internet users. That is consider whether past experiences have any effect on how internet users behave when they go online.

Our research shows that both awareness and preparedness only account for less than 10% of the variation of online behavior. It is therefore important to carry out further research in this area in order to determine the factors that majorly affect the On Line Behavior of the internet users.

References

1. Adams. A, Reich. P. &Weistein. S. (2012): "A Non – Militarized Approach to Cyber Security", *11th European Conference on Information Warfare and Security,*
2. Anderson. J. C & Coffey. D. (2010) "The United States: ICT Leader or Laggard" U.S. ICT Research and Development Policy Report, *Telecommunications Industry Association.*
3. Antwi-Bekoe. E. &Nimako .G.S. (2012) "Computer Security Awareness and Vulnerabilities: An Exploratory Study for Two Public Institutions in Ghana" *Journal of Science and Technology Vol.1 No. 7, July, 2012* pp 358 – 375
4. Aslanoglu. R &Tekir. S (2012):"Recent Cyberwar Spectrum and its Analysis", *11th European Conference on Information Warfare and Security,* The Institute EcoleSupèrieure en InformatiqueElectronique et Automatique, Laval, France 5 – 6 July 2012; Reading UK: Academic Publishing International Limited pp 45 – 52
5. Baharudin .S. A (2007): "Computer Abuse, Social Bond factor and the Role of Information and Communication Technology Deterrents as Moderator in the Malaysian Public Organizations". *Thesis Submitted in fulfillment of Doctor of Philosophy;* University of Malaysia.
6. Bhattacherjee, Anol, "Social Science Research: Principles, Methods, and Practices" (2012). *USF Tampa Bay Open Access Text books Collection.* Book 3. Available on http://scholarcommons.usf.edu/oa_textbooks/3 [Accessed on 14/12/2013]
7. Communication Commission of Kenya: Quarterly Sector Statistics Report; 4th Quarter April – June 2012/2013 Available on http://www.cck.go.ke/resc/downloads/Sector_Statistics_Report_for_3rd_Quarter_2012-2013.pdf[Accessed on 17/8/2013]
8. Communication Commission Of Kenya: Functions of the KE – CIRT/CC Available on www.cck.go.ke/industry/information_security/ke-cirt-cc/functions.html [Accessed on 17/8/2013]
9. "Comprehensive Study on Cybercrime" (2013): United Nations Office on Drugs and Crime (UNODC), *Draft Report 2013*

10. "Computer Crime Survey", (2005): *Federal Bureau of Investigation* Report of 2005. [online] Available on www.fbi.gov/publications/ccs2005.pdf [Accessed on 18/6/2013]
11. Contardor H, (2013): "African Union must act to reduce cyber crime" *International Data Group (IDG) Connect.*
12. Directorate of e-Government Kenya Web page (2011). Available on www.e-government.go.ke [Accessed on 25/8/2013]
13. Enders J. (2001): "Measuring community awareness and preparedness for emergencies" *Australian Journal of Emergency Management*
14. European Network and Information Agency (2006): "End User's Guide: How to Raise Information Security Awareness"
15. Global Project on Cybercrime, 2013: The cybercrime legislation of Commonwealth States: Use of Budapest Convention and Commonwealth Law Model.[online] Available on http://www.ceo.int/cybercrime[Accessed on 17/7/2013]
16. Gordon G.R, Hosmer C.D, Siedsma C, Rebovich D, 2003: Assessing Technology, Methods and Information of Committing and Combating Cyber Crime Available on http//www//ncjrs.org/pdffiles1/nij/grants/198421.pdf. [Accessed 15/7/2013]
17. Thompson H. (2002): "What Do We Really Understand When We Talk About Computer Crime?" *Trusted Information Management Ltd 2002*
18. IN VIA (2011): "Lost in the Cyber World – A project explaining the dangers harboured in the Internet" *Information for parent and educators Published by IN VIA in Berlin* (2011)
19. Israel .G.D (2009): "Determining the Sample size" *University of Florida.* Available on http://edis.ifas.ufl.edu [Accessed on 2/1/2014]
20. ITU Global Cybersecurity Agenda (GCA) High Level Experts Group (HLEG) Global Strategic Report (2008). Available on www.itu.int/cybersecurity/gca [Accessed on 15/8/2013]
21. Jellenc. E (2012):):"Explaining Politico – Strategic Cyber Security: The Feasibility of Applying the Arms Race Theory", *11th European Conference on Information Warfare and Security,* The Institute Ecole Supèrieure en Informatique Electronique et Automatique, Laval, France 5

– 6 July 2012; Reading UK: Academic Publishing International Limited pp 151 – 162

22. Kenya Demographic Profile (2013) Available on www.Indexmundi.com/kenya/demographic - profile html[Accessed on 10/12/2013]
23. Kenya ICT Board (2012): "Connected Kenya 2017; *National ICT Master Plan*" Available on www.ict.go.ke/docs/MasterPlan2017.pdf [Accessed on 10/7/2013]
24. Kenya launches National Cyber Security Strategy and Master Plan. [Online] Available onhttp://www.cio.co.ke/news/main-stories/kenya-launches-national-cyber-security-strategy-and-master-plan. [Accessed on 10/7/2013]
25. Keren & Elazari**, (**2012): "Internet as a CII – A Framework to Measure Awareness in the Cyber Sphere" *2012 4th International Conference on Cyber Conflict*. Czosseck. C, Ottis. R, Ziolkowski .K
26. Koops. B.J. (2011): "The Internet and its Opportunities for Cybercrime" *Tilburgy Law School Legal Studies Research Paper Series No 9/2011* [Online] Available on http://ssrn.com/abstract=1738223
27. Kothari C.R (2004): *Research Methodology Methods and Techniques*, (2nd Revised Edition.), New Delhi, New Age International Publishers.
28. Kumar & Ranjit (2005): *Research Methodology A Step – by – Step Guide for Beginners*, (2nd Edition), Singapore, Pearson Education.
29. KunzM. & WilsonP., 2004: "Computer crimes and Computer fraud". *Report to the Montgomery County Criminal Justice Commission.*
30. Lavraskas.P. J. "Encyclopedia of Survey Research Methods" Online ISBN 9781412963947 Available on srmo.sagepub.com/view/encyclopedia-of-survey-research-methods/n571.xml
31. LeFebvre. R (2012): "Human Element in Cyber Security: A study of Students Motivation to Act". *Paper submitted in the fulfillment of the requirements for the degree of Master of Psychology* Kennesaw State University.
32. Lewis A.J (2013): "Raising the Bar for Cybersecurity" *Technology and Public Policy*, Centre for Strategic and International Studies February 12, 2013

33. MagutuP.O, OndimuG. M &IpuC.J (2011): “Effects of Cybercrime on States Security: Types Impact and Mitigation with Fibre Optics Deployment in Kenya” *Journal of Information Assurance & Cybersecurity* Vol. 2011 20 pages.

34. Makatiani W. (2012):“Top 2012 Enterprise ICT Trends in Kenyan Business” *Kenya Cyber Security Report.* Available on http://www.cio.co.ke/news/main-stories/top-2012-enterprise-ict-trends-in-kenyan-business. [Accessed on 12/7/2013]

35. Makumi L.K. (2012): “An Analysis of IT Security and the Adoption of Security Policies: A Case Study of Kenyan Small and Medium Enterprises” *A paper submitted for fulfillment for the award of Masters of Science in Information System degree of the University of Nairobi in 2012.*

36. Maybury M, (2009): “Insiders Threats: Countering Cyber Crimes from within.” *Institute for Information Infrastructure Protection,* Dartmouth Colleg

37. Mesko, G &Bernik I (2008): “Cyber Crime: Awareness and Fear; Slovenian Perspective”, *Journal of Criminal Justice and Security* Vol. 5

38. Mugenda.O.M&Mugenda .A.G (2003): *“Research Methods: Quantitative & Qualitative Approaches”;* Nairobi, Kenya; African Centre for Technology Studies (ACTS)

39. Murungi (2012) “The Indonesian Job: Cyber law, Cyber Crime in Kenya – ICT and Telecommunication law in Kenya” Available on michaelmurungi.blogspot.com/2012/02/Indonesian-job.html [Accessed on 25/7/2013]

40. Ng K.K (2010): “Technology Solution to Fight Cybercrime” *Asia Pacific Regional Workshop on Fighting Cybercrime* Symantec Corporation

41. Olowu. D. (2009): “Cyber – Crimes and the Boundaries of Domestic Legal Responses: Case for Inclusionary Framework for Africa ”, 2009 (1) *Journal of Information, Law & Technology (JILT),* Available on http://go.warwick.ac.uk/jilt/2009_1/olowu [Accessed on 14/8/2013]

42. Pladna. B.(undated): “Lack of Attention in the Prevention of Cyber Crime and How to improve it” *ICTN6883 East Carolina University*

43. Ponemon Institute Research Report (2011): “Understanding Security Complexity in 21st Century IT Environments: A study of IT practitioners

in US, UK, France, Japan & Germany" *Sponsored by Check Point Software Technologies, Independently Conducted by Ponemon Institute LLC Publication Date February 2011*

44. Prakash. S, Vaish. A, Coul. N, Kumar. S, Srinidhi .T.N and Botsa. J (2013): "Child Security in Cyberspace Through Moral Cognition" *International Journal of Information Security and Privacy(IJISP)* Vol. 7, Issue 1
45. QuarshieH.O & Odoom A.M (2012):"Fighting cybercrime in Africa"; *Computer Science and Engineering* 2(6) 98 – 100.
46. Schmitt. N (1996): "Uses and Abuses of Coefficient Alpha"; *Psychological Assessment* Vol. 8 No. 4, 350 – 353
47. Schreier .F, Weekes .B & Winkler .T (2013): "Cyber Security: The Road Ahead" *DACF Horizon 2015 Working Paper No. 4*
48. Security experts warn Kenya faces growing cyber threat. Available onhttp://www.businessdailyafrica.com/Company%20Industry/Security%20experts%20warn%20Kenya%20faces%20growing%20cyber%20threat/-/539550/924274/-/vtsuf5z/-/index.html.[Accessed on 22/7/2013]
49. Sihanya. B. (2011): "Confronting Cybercrime in Kenya", Article appearing on *The Daily Nation newspaper on 8th April 2011* Available onhttp://www.innovativelawyering.com/blogs/6-ict-trade-and-corporate-governance-programme-profile[Accessed on 22/5/2013]
50. Solms. B. &Solms. R. (2004): "The 10 deadly sins of information security management" *Computers & Security (2004) 23, 371 – 376*
51. Smith. T.D (2011): "Cyber Crime: How it Happens and How you can Protect Yourself" New York State Office of Cyber Security Monthly Security Tips News Letter Vol. 6, Issue. 7
52. Thapa A& Kumar R (2011): "Cyber Stalking: Crimes and Challenges at the Cyberspace" *International Journal of Computing & Business Research;* Vol. 2, Issue 1, 2011
53. The Institute Ecole Supèrieure en Informatique Electronique et Automatique, Laval, France 5 – 6 July 2012; Reading UK: Academic Publishing International Limited pp 1 – 8
54. U.S. Department of Homeland Security (2012): "Homeland Security Grant Program; Supplemental Resource: Cyber Security Guidance"

55. Wall, D.S. (2003) “The Internet as a Conduit for Criminal Activity”, pp 77 – 98 in Pattavina, A (ed) *Information Technology and the Criminal Justice System*, Thousand Oaks, CA Sage (Revised March 2010)

56. Wamuyu. P. K. & Maharaj. M. (2011) "Factors influencing successful use of mobile technologies to facilitate Ecommerce in small enterprises: The case of Kenya," *The African Journal of Information Systems*: Vol. 3: Iss. 2, Article 2. Available at: http://digitalcommons.kennesaw.edu/ajis/vol3/iss2/2 [Accessed on 15/12/2013]

57. World Bank Report(2012): World Development Indicators “Internet users” Available on *http://data.worldbank.org/indicator/IT.NET.USER.P2*[Accessed on 7/6/2013]

58. Yamane (1967): *Statistics: An Introductory Analysis*, 2ndEd., New York: Harper and Row.

RESEARCH QUESTIONAIRE

The Data collected using this questionnaire is meant for academic research purpose only. The source of the information will be kept confidential.

This questionnaire is part of a research that seeks to establish the level of awareness and preparedness among the end users of the internet on issues of computer/cyber crimes. The two terms, i.e. Computer and Cyber crime can be used inter-changeably.

In this questionnaire, Computer crime is any criminal acts that involve computers and computer networks. Computer crime is not synonyms to **internet crime**, Computer crime has much wider expression encompassing - besides Internet, the computer and its networking, data present in digital form in the computer or on any storable device, software and hardware in any functional form. Computer crime can be committed even when one is offline.

Generally, **cybercrimes/internet crimes** are carried out by way of illegal access into another's data base, illegal interception, data interference, system interference, misuse of devices, forgery and electronic scams; they can be described as everything from electronic hacking to denial of – service attacks. As an internet user you are likely to have been a victim without your knowledge. It is likely that you have been receiving junk mail in your in box or worse of someone has been sending mails to your contacts in your name. These are part of the issues that this research is intending to look at.

Section A: Respondent Information

Please tick appropriately using [√] in the square brackets provided:

1. Please indicate your gender?

   Male [ ] Female [ ]

2. What is your highest level of education?

   Postgraduate [ ], Bachelor's Degree [ ], Diploma [ ], Others [ ]

3. Age in years: 18 – 22 [ ], 23 – 27 [ ], 28 – 32 [ ],
   33 – 37 [ ], Above 38 [ ]

Section B: Background Information

1. Do you always surf the internet? Yes [ ], No [ ]

2. What do you normally use when surfing?(Device can be more than one)

   Personal Computer [ ] Office Computer [ ]
   Commercial (Cyber) café [ ] Personal Mobile phone [ ]

3. Which of the following activities do you carry out online? (You can choose more than one activity)

   Checking and replying Emails [ ] Socializing [ ],
   Research [ ], Shopping [ ],
   Search of information [ ], Downloading Music & Movies [ ],
   Gambling [ ], Banking [ ],
   Auction [ ],
   Any others (Please specify)

   ____

4. How long have you used computers?

   Below 1 year [ ], 1-3 years [ ], 4-6 years [ ],
   7-9 years [ ], Over 10 years [ ]

5. Have you ever attended any formal computer training course/ seminar/ workshop?

   Yes [ ], No [ ]

6. As an internet end user are you aware of the existence of computer crimes?

   Yes [ ], No [ ]

7. If the answer to Question 6 above was yes, where did you first hear about computer crimes?

   From Mass Media [ ], From a friend [ ], From a computer course [ ], From a family member [ ] Other sources (Please specify)________________________

8. Have you ever been trained on computer-related threats and crime?

   Yes [ ], No [ ]

9. How often do you hear people talking/discussing computer crime issues?

   Very Often [ ]   Often [ ]   Rarely [ ]   Never [ ]

Section C:

Knowledge about Computer Crimes (KCC)

Please indicate your level of agreement with the following statements by ticking the appropriate box:

Key: Strongly Agree (**SA**); Agree (**A**); Neutral (**N**); Disagree (**D)** Strongly Disagree (**SD**)

No.	**Statement**	**SD**	**D**	**N**	**A**	**SA**
KCC 1	There are risks involved whenever I am working online.					
KCC 2	I am aware of the various computer crimes I am likely to be exposed to while working online.					
KCC 3	It is always advice able to log in as a user rather than an administrator whenever going on line.					
KCC 4	There is no risk in using the same password for different accounts.					
KCC 5	I need to change my password regularly/frequently.					
KCC 6	Any password I use should have at least eight characters which should be a combination of alphabets, digits & symbols.					

Attitude to risks of Computer Crime (ACC)

No.	**Statement**	**SD**	**D**	**N**	**A**	**SA**
ACC1	I have no problem sharing my password with someone else.					
ACC2	I have no problem if someone is looking over my shoulder as I key in my password.					
ACC3	I should use the same password for different					

	accounts.					
ACC4	I should have authentication before accessing information in my computer.					
ACC5	I have no problem with unauthorized copying of data or information.					

Exposure to Awareness Raising (EAR)

No.	**Statement**	**SD**	**D**	**N**	**A**	**SA**
EAR 1	I have been getting information on computer-related threats and crime from the media					
EAR 2	There is need to attend formal training in computer to be able to avoid computer crimes					
EAR 3	Institutions of learning should make it mandatory to learn about computer crimes					
EAR 4	I have no problem downloading Free Software and then copying the same to a friend.					
EAR 5	It is important to control the access of others to my computer by using different User Account.					
EAR 6	All web sites should block my account when they see a large number of failed login attempts.					

Preparation to Respond (PR)

No.	**Statement**	**SD**	**D**	**N**	**A**	**SA**
PR 1	I should only have Genuine operating system installed on my computer.					
PR 2	Firewalls and antivirus should be necessary features in my personal computer (PC) whenever going online.					
PR 3	I should update both the antivirus and operating system installed in my PC at all					

	times.					
PR 4	Apart from the antivirus installed in my PC, another kind of security program should be added.					
PR 5	I should do a full system anti-virus scan on my PC at least once in a week.					
PR 6	I need to backup my data regularly so as to avoid data loss in case of a computer crash.					

Online Behavior

No.	**Statement**	**SD**	**D**	**N**	**A**	**SA**
OB 1	I should spam all emails from people I do not know.					
OB 2	I should always open emails with attachment from a person that I know.					
OB 3	I should comply with pop-up messages from my Internet Service Provider (ISP) providing a linking's for verification or update account information.					
OB 4	I should ignore pop up messages on the screen when online informing me that I have won some money and inviting me to click on a link provided.					
OB 5	I should allow the browser to store my password in order to ease accessing the net.					

D: Computer Crime Incidences Experienced

1. Among the following computer incidences which one has you experienced within the last one year? (**The incidences can be more than one)**

Spam mail [ ], Denial of Service [ ],
Hacking [ ], Identity theft [ ],

Computer crashing [ ], Theft of computing device [ ],

Virus or worm attack [ ] Trojan or rootkit attack [ ]

Any other (Please specify)____-

____

2. For each of the incidences listed above indicate (**with a number**) the frequency of occurrence of each of them within the last one year.

Spam mail [ ], Denial of Service [ ],

Hacking [ ], Identity theft [ ]

Computer crashing [ ], Theft of computing device [ ],

Virus or worm attack [ ], Trojan or rootkit attack [ ]

Others (**Please Specify the incidence and the number of times)**

____

Thank you for taking your time in answering this questionnaire