EFFECTIVENESS OF ONLINE SAFETY AWARENESS CAMPAIGN STRATEGIES BY KENYA BANKERS ASSOCIATION ON SMALL BUSINESS OPERATORS IN KASARANI SUB-COUNTY, NAIROBI

BY

PETER K. OMUSULA

UNITED STATES INTERNATIONAL UNIVERSITY OF AFRICA

SUMMER 2022

EFFECTIVENESS OF ONLINE SAFETY AWARENESS CAMPAIGN STRATEGIES BY KENYA BANKERS ASSOCIATION ON SMALL BUSINESS OPERATORS IN KASARANI SUB-COUNTY, NAIROBI

BY

PETER K. OMUSULA

A Thesis Submitted to the School of Communications, Cinematic and Creative Arts in Partial Fulfilment of the Requirement for the Degree of Master of Arts in Communication Studies

UNITED STATES INTERNATIONAL UNIVERSITY OF AFRICA

SUMMER 2022

DECLARATION

I, the undersigned, declare that this is my original work and has not been submitted to any other college, institution or university other than the United States International University-Africa for academic credit.

Signed: _____ Date: _____

Peter K. Omusula (Student ID No. (649148)

Signed: _____ Date**: 6/9/2022_**

Dr. Joseph N. Nyanoti

Supervisor

Signed: _____ Date: _____

Dr. Dorothy W. Njoroge, Ph.D.,

Chair, Department of Media and Communication

Signed: _____ Date: _____

Dean, School of Communication, Cinematic and Creative Arts

COPYRIGHT

ACKNOWLEDGEMENT

I wish to appreciate the support given by different people to make this work possible. I would not have produced this thesis without their contribution. Unfortunately, I cannot list all the names, but I can appreciate each individual who contributed to the success of this work. Just to mention a few, I would like to acknowledge United States International University of Africa for allowing me to study while working and for financial support.

I am also grateful to my University Supervisor Dr. Joseph Nanyoti for guidance and useful comments throughout the study process. Without him, this work could not be what it is. In addition, I wish to thank the entire staff of Media and Communication Department, and School of Communication, Film, and Creative Arts, who in one way or another provided guidance and relevant information that led to production of this thesis.

Lastly, I wish to thank respondents for providing relevant information that enabled me to come up with this thesis. Without their information, this thesis could not be what it is. To all I say thank you.

DEDICATION

This work is dedicated to my wife, Eliza Wanjiru, My daughters Ann Wanjiru and Vanessa Nandwa, My dad, late mum, sisters and brother.

TABLE OF CONTENT

COPYRIGHT ..... **iii**
ACKNOWLEDGEMENT ..... **iv**
DEDICATION ..... **v**
LIST OF TABLES ..... **viii**
LIST OF FIGURES ..... **ix**
LIST OF ABBREVIATIONS AND ACRONYMS ..... **x**
ABSTRACT ..... **xi**
CHAPTER ONE **1**
1.0 Introduction **1**
1.1. Background to the study 1
1.2. The Statement of the Problem 4
1.3. The Purpose of the Study 6
1.4. The Objectives of the Study 6
1.5. Research Questions 6
1.6. The Significance of the Study 7
1.7. Scope of the study 8
1.8. Definition of terms 8
1.9. Chapter Summary 9
CHAPTER TWO **10**
LITERATURE REVIEW **10**
2.0 Introduction 10
2.1 Theoretical Framework 10
2.2 General Literature Review 14
2.3 Empirical Literature 17
2.4 Conceptual Framework 24
2.5 Chapter Summary 25
CHAPTER THREE **26**
METHODOLOGY **26**
3.0 Introduction 26
3.1 Research Design 26
3.2 Research Approach 26
3.3 Study Area 27

3.4 Population and Sampling 27
3.5 Sampling Procedure 27
3.6 Data Collection Methods and Instruments 28
3.7 Data Processing and Analysis 30
3.8 Ethical Considerations 30
3.9 Chapter Summary 30
CHAPTER FOUR 32
FINDINGS AND ANALYSIS 32
4.1 Introduction 32
4.2 Response Rate 32
4.3 Reliability of the Study 32
4.4 Background Information of the Respondents 33
4.5 Research Objective 1: How Small Business Operators in the Kasarani sub-County have adopted the use of ICT in their Businesses 36
4.6 Objective 2: To assess cybercrime awareness among the small business operators in Kasarani sub-county, Nairobi. 39
4.7 Research Objective 3: To assess the effectiveness of Strategies employed by the Kenya Bankers Association initiative "Kaa Chonjo" in curbing cybercrime 41
4.8 Intervening Variable Analysis – Media Strategies Impact on Kenya Bankers Association campaign and Cybercrime Awareness 44
4.9 Chapter Summary 49
CHAPTER FIVE 50
DISCUSSIONS, CONCLUSIONS, AND RECOMMENDATIONS 50
5.1 Introduction 50
5.2 Summary of Findings 50
5.3 Discussion 52
5.4 Conclusions 54
5.5 Recommendations 55
5.6 Areas for Further Research 56
REFERENCES 57
APPENDIX I: QUESTIONNARE 65
APPENDIX II:IRB LETTER 69
APPENDIX III: NACOSTI LETTER 70

LIST OF TABLES

Table 4.1: Response rate 32
Table 4.2: Reliability of the Study 33
Table 4.3: Awareness of Cybercrime Issues 40
Table 4.4: Kenya Bankers Association Campaign 42
Table 4.5: Correlation between Cybercrime awareness level and Kenya Bankers Association campaign 43
Table 4.6: Regression Analysis; Kenya Bankers Association campaign versus Cybercrime awareness level 43
Table 4.7: Analysis of Variance (ANOVA); Kenya Bankers Association campaign versus Cybercrime awareness level 44
Table 4.8: Descriptive Statistics; Media Strategies 45
Table 4.9: Kenya Bankers Association initiative vs. cybercrime awareness 46
Table 4.10: Regression Analysis: Media Strategies versus Kenya Bankers Association campaign 47
Table 4.11: ANOVA; Media strategies impact versus Kenya Bankers Association campaign 47
Table 4.12: Correlation Analysis; Media strategies versus cybercrime awareness 48
Table 4.13: Regression Analysis; Media strategies versus cybercrime awareness 48
Table 4.14: Analysis of Variance (ANOVA); Media strategies impact versus cybercrime awareness. 49

LIST OF FIGURES

Figure 2.1: Adopted from Technology Acceptance Model from Davis, Bagozzi, eta al Warshaw (1989) 13
Figure 2.2: Conceptual Framework. Source: Author (2019). 24
Figure 4.1: Gender of Respondent 33
Figure 4.2: Respondents' Age Bracket 34
Figure 4.3: Highest Level of Education 35
Figure 4.4: Length participant has operated their business in the Kasarani constituency 35
Figure 4. 5: Trained on computer-related threats and crime 36
Figure 4.6: Mobile phone usage in small businesses 37
Figure 4.7: Purpose of the Mobile Phone in Businesses 38
Figure 4.8: Cybercrime incidences experienced 39

LIST OF ABBREVIATIONS AND ACRONYMS

APT – Advanced Persistent Threat

CAK – Communication Authority of Kenya

EU- European Union

EULA- End User License Agreement

KBA- Kenya Bankers Association

OS- Operating System

SMS- Short Message Services

UNEP- United Nations Environmental Program

PC- Portable Computers

ABSTRACT

This study examined effectiveness of online safety awareness campaign by Kenya Bankers Association (KBA) to small business operators in Kasarani Sub-county Nairobi. The Key objectives of the study were to examine the extent to which small business operators in Kasarani sub-county have adopted use of ICT in their businesses, assess their cybercrime awareness levels, and the effectiveness of strategies employed by the Kenya Bankers Association initiative "Kaa Chonjo" in curbing cybercrime. Kasarani Sub-County where the study was done has more small businesses operating online than any other sub-county in Nairobi; hence it was an ideal site for the study. Relevant theoretical and empirical literature relevant to study area was reviewed. This study used survey research design. Multi-stage sampling was used to select the study area and sampling units. Whereas purposive sampling was used to select the study area, stratified random sampling was used to select sample units from different small businesses. Total sample size was 335. Structured questionnaires were used to collect data. Data captured was summarized, analyzed and presented using SPSS version 25.0 in that order. It was evident from the study that most small business operators have adopted use of ICT in the businesses specifically use of mobile phones. However, majority (60%) of the small business operators have not had any training on cybercrime awareness. On awareness about cybercrime, most small businesses were found to have experienced cybercrime. The study found out that there was a relatively strong relationship between the online safety campaign strategies by KBA and cybercrime awareness among small business operators in Kasarani. Mass media came out as the most effective strategy in cybercrime campaigns as compared to other strategies. This study recommends that the KBA to employ more use of mass media campaigns as a strategy of reaching out to more small business operators in the study area.

CHAPTER ONE

1.0 Introduction

The chapter discusses use of information and communication technology for development as a form of development for communication. Small, medium and large business entities rely on new technology to operate effectively. However, reliance on new technology exposes these business entities to cyber-attacks.

The large, and medium sized entities are well prepared to deal with cyberattacks, as compared to small businesses that do not have financial muscles to invest in cybersecurity (Aiken et al., 2016). Since many small businesses in Kenya rely on cyber space as a platform for transacting their businesses, the current study intends to establish the effectiveness of the Kenya Bankers Association initiative dubbed “Kaa chonjo” on cybercrime awareness of the small business operators in Kasarani Sub County.

1.1. Background to the study

Use of Information and communication technologies for development (ICT4D) is the contemporary form of communication for development. According to Kamel (2005), this concept refers to the role that new technologies, in particular digital media, play in development communication to empower people and further advance the overall development project. OECD (2004) states that use of information and communication technology is widespread in businesses of all sizes. In addition, Covid-19 has seen so many businesses move to online platforms, which has resulted to alarming rate of cyberattacks (Khan & Mkuruzangwe, 2022). Reported cybercrime in Kenya, increased to 140 million in 2022 which represents 40 percent increase as compared to previous year (Statista, 2022).

According to Communication Authority (2019), cyberattacks have narrowed down to small businesses after big companies developed adequate security checks which minimized the chances of being attacked. The Report further indicates that the perpetrators target vulnerable groups who use mobile phones. In Kenya, Statista (2022) notes that as of May 2022, most of the web traffic occurred via mobile devices which had 73 percent share of the total traffic, as compared to access to the internet other devices. Communication Authority (2021), quarterly statistics report covering July to September 2020 indicated further that there was a sharp increase of cyber threats during the period with 35.1 million incidents in Kenya representing 152.9 percent Jump. Communication Authority (2021) and Rotich (2021) are in agreement that this increase in cyber-attack is attributed to the move to working remotely and increased uptake of e-commerce in response to covid-19 pandemic in Kenya.

Armin et al (2015) in their survey, sought to establish if their respondents had experienced a cybercrime attack in the previous five years. They found out that 78 percent of the respondents had experienced cybercrime. Furthermore, they observed that cybercrime was among the top five crimes in European Union National Security Strategy in the last five years. Armin et el. (2015) argued that when cybercrime is compared to property crime, it was not easy to come up with the metrics. In other words, it was easier to come up with the cost of property crime to United States of America's economy, but there was no direct answer for the cost of cybercrime on any economy of a given country. Amin et el (2015) elaborate further on this situation that the cost of cybercrime to global economy is estimated to be more than 300 billion Euros. Furthermore, cybercriminals collect revenues worthy 15 billion Euros per annum. This is because about 3 billion people use internet which is about 39 percent of global population. It is estimated that there are 2.3 billion mobile phone users subscribed worldwide (Statista, 2019).

In Serianu's Cybersecurity report (2016) as quoted in Karibu (2018), African countries lost at least $2 billion in cyber-attacks in 2016. According to Karibu (2018), the estimated cost of cybercrime in Kenya stood at $210 million, and Nigeria led the pack in Africa with estimated cost of cybercrime in 2017 being $649 Million. The rise in cybercrime attacks in African counties, can be attributed to what Ksherti (2019) refers to as high rate of computerization of processes, vulnerable systems and lax cybersecurity practices, and lack of skills among internet users to protect themselves from cyber threats.

Although most cybercrime fraud affects small businesses and organizations which have invested less in cybersecurity, internet use puts individual users at risk of cybercrime (LeFebvre, 2012). NG (2010) observes that the human factor is the weakest link in cybersecurity. The human side is easily exploited and constantly overlooked by the experts as well as policy makers. Alluding to this fact, Finaccess (2019) noted that nearly 30 percent (over 5 million users) of mobile money users experienced loss of money or fraud mostly through hoax, SMSs or phone calls.

According to Kenya Bakers Association (2018) the basic mitigation measures against the ever-growing problem of cybercrime is awareness creation among the cyberspace users. The Kenya Bankers' Association (2018) further observed that computer use and vulnerability to cybercrimes are major factors that need to be communicated to all individuals. It is on this basis that the Kenya Bankers Association (KBA) put in place an initiative dubbed "be alert"/ "Kaa chonjo" to curb cybercrime. The initiative seeks to empower consumers of financial services with information to secure use of online, mobile, and card transactions besides contributing to alleviating fraud in financial sector (Koigi, 2018). This campaign came on the backdrop of rising economic fraud targeting both financial institutions and consumers. The current study will assess the effectiveness of

online safety awareness campaign strategies to small business operators by Kenya Bankers' Association in Kasarani Nairobi County.

1.2. The Statement of the Problem

Most small businesses rely on technology to help them operate. Brookins (2019) observed that technology has the potential to affect small business in positive and adverse ways, depending on the goals a business has in place, the products they chose to use, and how well entrepreneurs and their employees adapt to new systems. Brookins (2019) noted further that through technology business owners can work remotely, hire talents globally, provides instant connection to the potential customers, provide trainings, and access online payment options among other services. Kemb (2022) indicates that there were 23.35 million internet users in Kenya in January 2022, and internet penetration rate stood at 42.0 percent of the total population at start of 2022. Statista (2019) points out that majority (74 per cent) of web traffic in African market originated from mobile devices.

This increase in penetration of the internet is good for the businesses that have adopted the use of new technology. However, Jones, Chin, and Aiken (2014), observed that this increase is a huge contributing factor to the rising cases of cybercrime; which has effect on how businesses are done. Evidence indicates that small businesses experience more online threats than larger businesses primarily due to the lack of investment in cybersecurity protection plans (Aiken et al., 2016). The fact that cybercrime is still growing in terms of numbers and finanicial loses suggests that existing approaches are still inadequate (Shah, Jones, & Choudrie, 2019).

A number of researches have been done globally on effectiveness of awareness campaigns on the cybserspace users. Among them we have Bada, Solms, and Agrafiotis, (2012) who carried a study in reviewing national cybersecurity awareness in Africa. They

found out that African countries do not posses a national programme for raising awareness. In United Kingdom and South Africa, Kritzinger, Bada, and Nurse, (2017) study focussed on cybersecurity awareness initiatives for school learners in South Africa and the UK. They recommended a national plan for the countries to improve on cybersecurity awareness for learners.

In Kenya both small and large scale businesses heavly use internet in carrying out their activities. As a result, most businnesses are exposed to cyberattacks. Okuku, Renaud, and Valeriano (2015), carried out a research on the role of governmental cybersecurity strategy and explored the approaches to be used for improving public awareness of mobile internet threats. They found out that there was need for the government to roll out awareness campaigns targeting all sectors of society using mobile internet.

In a study by Nzeakor, Nwokeona, and Ezeh (2020), "Patterns of Cybercrime in Imo State, Nigeria," they found out that the level of cybercrime appeared to be very high (N=915; 89%), the level of cybercrime also appeared to be superficial because majority (78%; N=804) of the respondents appeared only to be aware of the computer focused cybercrime. The study also found out that the level of awareness appeared to be gender sensitive since more males appeared to be aware than the female respondents. They recommended that more focused cybercrime awareness focused on females and children need to be embarked upon by the stakeholders.

From the above reviews, there exists a knowledge gap on the effectiveness of cybercrime awareness initiatives/campaigns in curbing cybercrime. Nzeakor, Nwokeona and Ezeh (2020) study indicates further that cybercrime awareness should also be more focused to the strata of people in the society who are not aware about it. It is against this backdrop that the current study intends to examine the effectiveness of one such initiative

by Kenya Bankers Association dubbed “Kaa Chonjo” on cybercrime awareness among small business operators. This study seeks to fill this gap. If the cybercrime awareness creation to small business operators will not be done, more business will close down due to cybercrime threat.

1.3. The Purpose of the Study

The purpose of this study was to examine the effectiveness of KBA’s annual initiative “Kaa chonjo” in creating cybercrime prevention awareness among small scale business operators.

1.4. The Objectives of the Study

The main objective of the study was to examine effectiveness of KBA’s annual initiative on public awareness about prevention of cybercrime with an aim of proposing strategies that could be used to foster cybercrime awareness among small scale business owners in Kasarani Sub-county.

The specific objectives are:

1. To examine the extent to which small business operators in Kasarani sub-county have adopted use of ICT in their businesses
2. To assess cybercrime awareness among the small business operators in Kasarani sub-county, Nairobi.
3. To assess the perceptions of small business operators on the effectiveness of strategies employed by the Kenya Bankers Association initiative “Kaa Chonjo” in curbing cybercrime.

1.5. Research Questions

The following research questions guided this study:

1. How have the small business operators adopted use of ICT in their businesses in Kasarani Sub-county?
2. To what extent are the small business operators in Kasarani Sub-county aware about cybercrime prevention?
3. How effective are the strategies employed by the KBA's initiative on cybercrime prevention among the small business operators?

1.6. The Significance of the Study

The study is of great value to small-scale businesses that make use of ICT in their daily transactions. It gave practical insights in cyber threats and cyber security management, especially the need to implement more effective cyber threat countermeasures on cyberspace users.

The study contributes to academic knowledge on cyber security threats; cyber threats countermeasures and cyber security. It provides to academicians, scholars and researchers with additional written material on the concepts of cyber security threats, cyber threats countermeasures and cyber security. The study offers cyber security development with better answers to take care of the worries and necessities of their clients.

The study was important to the small-scale business owners as it sheds more light regarding the cyber threats that they are facing. This helps in gauging the level of public awareness creation hence suggest areas that require improvement.

Further, the study came up with recommendations on how to handle the cybercrime issues that are of great help to the government and the ministry of Information, Communication and Technology.

1.7. Scope of the study

The research examined the extent to which small business operators' in Kasarani area have adopted use of ICT in their businesses, their understanding of cybercrime and effectiveness of the KBA's annual initiative on fighting incidents of cybercrime. The study limited itself to the above objectives.

The study employed use of a survey method. The study targeted small business operators within Kasarani, Nairobi County because they majorly depend on mobile phones to transact their businesses.

1.8. Definition of terms

Cybercrime in this study refers to the use of a computer to commit a crime.

Cyberattack in this study refers to an attempt to gain unauthorized access to the computer, computing system, computing network with a view to cause damage.

Entrepreneur is a person who attempts to make a profit by starting a company or operating alone in business world especially when it involves taking risks.

Small business in this study will refer to types of small business with single owners or fewer employees and requiring small capital to operate

Kaa Chonjo is a Swahili phrase which means to be alert. In this study is used to mean awareness about cybercrime.

Internet safety refers to the art of staying safe online. In this study refers to the art of small business operators remaining safe online.

Mass media refers to communication either written, oral or spoken that reaches larger audience. For this study refers to radio stations, Television stations and Newspapers.

Hacking in this study refers to unauthorized access to computing devices with intention to cause damage.

Identity theft in this study refers to a form of crime where an attacker uses fraud or deception to obtain personal information or sensitive information from a person and misuses it to act in victim's name. Example are social engineering and phishing.

Data theft in this study refers to the act stealing information stored on someone's devices such as computer database, smartphone storage etc.

1.9. Chapter Summary

This chapter has presented an introduction to the study, and background of the study. The background indicates that cybercrime has greater impact on today's operations than a decade ago due to dependency on virtual world. As a result the cybercrime threats are on the rise. However, the Kenya Bankers Association is currently carrying out an initiative to create awareness among cyberspace users on their safety while online. This study is significant because it will add value to the small business operators who transact most of their day today's transactions online. The chapter has definition of terms and a summary.

The next chapters covers literature review pertaining to the research topic. The literature is reviewed based on the research objectives highlighted in chapter one. Chapter three presents research methodology that will be used in the study.

CHAPTER TWO

LITERATURE REVIEW

2.0 Introduction

This chapter has theoretical framework, literature review and the chapter summary. The study adopted Diffusion of Innovation (DOI) Theory and Technology Acceptance Model to explain the effectiveness of Kenya Bankers Association annual campaign initiative on cybercrime awareness. A summary of the literature review in existence, both general literature review, and empirical literature has also been done. The summary has been done as per the objectives of the study, which are: To examine how small business operators in Kasarani have adopted use of ICT in their businesses, assess their awareness of cybercrime, and examine the effectives of strategies employed by the Kenya Bankers Association annual initiative "Kaa Chonjo" in curbing cybercrime. The relevant gaps in literature have been highlighted as well.

2.1 Theoretical Framework

The study adopted Diffusion of Innovation (DOI), and Technology Acceptance Model (TAM) as a basis for analysis. Both DOI and TAM share a similar premise that adopters assess innovation on the perception of their characteristics, or postulates that innovations having favorable features are likely to be more adopted (Al-Rahmi, et al., 2019, p.26798). Al-Rahmi et al (2019) observed further that value oriented aspects including perceived usefulness and relative advantage, effort oriented features for example perceived ease to use and complexity, compatibility are repeatedly been observed as major reasons manupulating adoption of inventions. These theories provide a clear link between variables as earlier researched by the scholars.

2.1.1 Diffusion of Innovations Technology

The proponent of this theory was Everet Rogers, a professor of communication studies in 1962. In his theory Rogers (2003) as quoted by Nazari, Khosravi, and Babaihavaeji, (2013) defines diffusion as "the process by which an innovation is communicated through channels overtime among members of a social system." Lamorte (2019) concurs with Naziri, Khosvari and Babaihavaeji (2013) definition. The perceived attributes of an innovation can help in understanding the rate of innovations. Rogers describes these factors in five categories of innovation attributes, namely: a relative advantage, complexity, observability, triability and perceived compatibility (Naziri, Khosvari, & Babalhavaeji, 2013; Al-Rahmi, et al., 2019).

A relative advatange refers to the level to which people assume that the new technology is better than the old traditional one. Thus, this term is used in the current study to refer to the degree to which small business operators believe that the use of online platform can enhance their businesses. Al-Rahmi, et al. (2019, p.26798) observed that the findings that the intention to use a system by the perceived advantages has frequently been reported.

Complexity refers to the level of difficulty in understanding innovations and their ease of use that is perceived by the end user. Based on thse definition, the current study uses this term to refer to extent of difficulty viewed by the small business operators to use the online platforms.

Triability is the extent to which the people think that they need to experience the innovation before taking the decision to adopt it. As for the current study, this concept refers to how a business operator views his or her use of online platforms to do business. Reseach done in the area of TAM and DOI found out that there is significant effect of perceived

use of the systems on obervabilty by users Al-Rahmi, et al., (2019). Observality has a positive impact on other dimensions such as perceived ease of use, behaviour intention to use the platform and usefulness.

Perceived compatibilty refers to the fact in which small business operators feel that the innovation is compatible with their standards, previous involvements and the desires of probable adopters.

Observabilty is the degree to which the outcome of an innovation is noticeable by others. The easer individuals can see the results the more they are able to adopt an innovation. The perceived observabilty is directly related to the rate of adoption of an innovation.

It can therefore be argued by this study that an innovation that is perceived by individuals as having greater relative advantage, compatibility, triability, observability and less compatible will be adopted more rapidly (Nazari, Khosvari and Babaihavaeji, 2013). However, in this context, because of differences in personal experiences, level of education, types of businesses etc, and small business operators will perceive use of online platforms differently.

This theory will be useful in explaining how various small businesses have adopted use of ICT in their operations. It will also be helpful in explaining how various small businesses have adopted the campaign initiatives by Kenya Bankers Association in preventing cybercrime attacks in their business.

However, the above theory works better with adoption of new behavior, idea or product rather than cessation or prevention of a behavior. This theory will be helpful in explaining the adoption of new technology in small businesses. However, the key KBA's campaign initiative is to ensure that people who have adopted use of technology are able to

reduce risks associated with the adopted technology. Technology Acceptance Theory (TAM) will be used to complement these weaknesses of DOI.

2.1.2 Technology Acceptance Model (TAM)

Technology Acceptance Theory was put forward by Davis in 1989. According to Charness, and Boot (2016), and Chen, Rong, Ma, Qu, and Xiong, (2017), TAM is one of the influential model to explain technology acceptance, with two primary factors influencing an individual's intention to use new technology: perceived ease of use and perceived usefulness. They argued that an older person who perceives digital games as too difficult to play or a waste of time will be unlikely to want to adopt this technology, while an older adult who perceives digital games as providing needed mental stimulation and as easy to learn will be more likely to want to learn how to use digital games. See figure 1

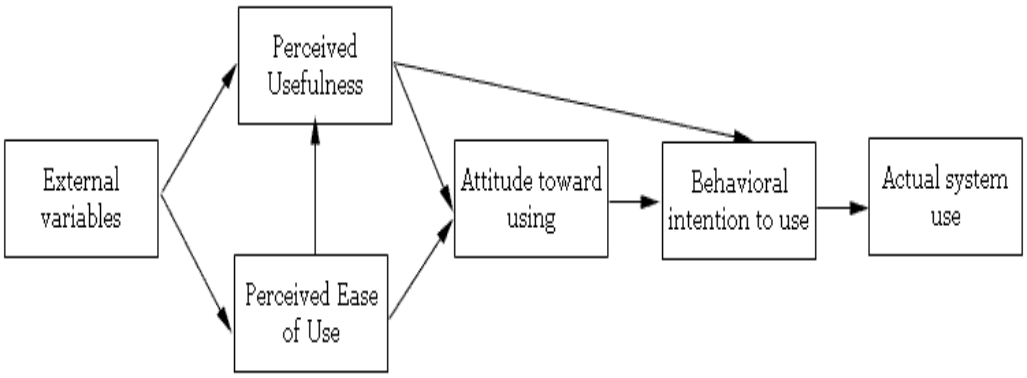

Figure 2.1: Adopted from Technology Acceptance Model from Davis, Bagozzi, eta al Warshaw (1989)

This model was helpful in explaining user behaviors towards preventing cyberattacks on the devices that they are using to transact their businesses after KBA's campaigns initiatives. This theory helps to explain if the small business owners have adopted cybercrime prevention measures as a result of the above campaigns by Kenya Bankers Association.

2.2 General Literature Review

2.2.1 Adoption of Mobile phones in small businesses

It was estimated that in the year 2019, 53.6 percent of the global population, or over 4.1 billion people were using internet (ITU, 2019). According to Statista (2022) report titled the Global Digital Population as of April 2022, there were 5 billion internet users worldwide, which is 63 percent of the global population. Of this total, the report indicates further that 6.45 billion or over 93 percent were social media users. Statista (2022) report global internet access via devices indicated that during the fourth quarter of 2021, more than 92 percent global users' accessed internet via any kind of mobile phone, while almost 91 percent accessed via a smartphone. In reference to Kenya, Communication Authority (2022) quarter report covering January to April, about 59 million mobile devices were connected to the mobile network for quarter ending September 2021, putting the penetration level to 67.9 percent.

The successful entrepreneur, enabled by mobile phone, plays a prominent role in the global development narrative and becomes a semi-regular fixture in the popular press (Economist, 2005). The mobile phones allow people to communicate at a distance and exchange information on real-time in the process increasing business productivity, business operators use mobile phone to serve existing customers more effectively, and in a new business venture, check market prices and bypass middlemen who carries goods to market. These use have significant implications for topics of interest to the development community, including the changing role of the informal sector and small enterprise in developing economies, our ideas about entrepreneurship and livelihoods, and our understanding of the informational society as a whole (Castells, 1996).

2.2.2 Cybercrime and Small Businesses

According to Morgan's (2019), Official Annual Cybercrime Report, there were averagely four billion internet users in 2018 up from two billion in 2015 globally. The report projects that there will be six billion internet users in 2022, globally. Internet World Stats (2019), estimates that in Kenya, Internet usage statistics was at 43, 239 43 by the end of May 2019. Most of the internet users access internet using smartphones (Berry & Berry, 2018). As global society is facing an ongoing digitization, the more cybercrime victimization has increased for both individuals and businesses (Weijer, Leckfeldt, and Zee, 2021, p.303). In Netherlands for example Weijer, Leckfeldt, and Zee (2021), noted that 3 percent of citizens are reported to have been victims of cybercrime in 2019. The most common crimes in their case were consumer fraud and hacking with victimization rate of 4.6 percent and 5.5 percent. Weijer, Leckfeldt and Zee (2021), noted that victimization rate in Netherlands is even higher among businesses at 28 percent of small and medium sized businesses being victims.

Communication Authority (2019) observes that smartphone penetration is at 60 percent of the population. As a result, people use mobile phones in one way or the other. However, newly produced mobile devices are very weak in security, such that criminals may easily hack such devices. Morgan (2016) indicates that just like street crimes, which historically grow in relation to population growth, we are witnessing a similar evolution of cybercrime. As a result of this growth, cybercrime has been on the rise because of the high penetration of internet in Kenya as compared to the rest of countries in Africa. Communication Authority of Kenya's (CAK) first quarter report for 2018/2019 shows that the National Cybercrime Centre detected 3.82 million cyber-attacks, a rise from 3.46 million reported in the last quarter of 2018. Norton report as cited by Mutisya (2019)

observes that most of cybercrime in Kenya target banking sector followed by government organizations.

Cybercrime is continuously targeting the small businesses and this is due to the vulnerabilities that they are presenting. The position that the small business have in terms of being economic drivers makes them one of the lucrative industries for the cybercrime due to amounts of money that is found within their operations. Furthermore, the target that is aimed at the small businesses is because they readily provide access information when it comes to personal information that belongs to their clients. The small businesses are also characterized with weak security systems and thus making it easier for the criminals to target their systems. The poor security can be attributed to the lack of financial resources to purchase strong security (Renaud, 2016). Serianu's Norton Cybersecurity Insights Report as cited by Mutisya (2019) points out that overconfidence by users and lack of cybersecurity strategies are exposing many small business operators to cybercrime. Muhati (2018) concurs with Mutisya (2019) that three-quarters of employees in formal sector have experienced cybercrime, but they don't have resources for cybersecurity making them prone to the attack.

The Serianu's Norton Cybercrime Insights Report indicates that when it comes to hacking, small businesses are the most prone (7 per cent) followed by medium (6 per cent), micro (5 per cent), and large businesses at 4 per cent. This observation concurs with Weijer, Leckfeldt, and Zee (2021). Besides, one in six incidents of cybercrime in private sector targets transportation section, storage, and health sectors. It is on this basis that the current study will focus on the small business operators in the study areas and how the KBA annual initiative "Kaa chonjo" has influenced their cybercrime prevention skills.

2.2.3 Kenya Association of Bankers Strategies to fight Cybercrime

The KBA's strategy in creating cybercrime awareness includes having an annual strategic communication plans designed to drive awareness and enhance the visibility of the campaigns, proactive activities to reach out to the target population and educating the public. These strategies have been activated through use of integrated publicity with digital, print and broadcast media as one front as well as dissemination of KBA's Information, Education and Communication (IEC) materials and events for people to seek more information and take action.

According to Kenya Bankers Association (2012), for example 21 articles were published in print media, 29 out of 32 banks were involved, IEC material distributed in police stations countrywide, 3 radio stations aired free spots, 19000 fliers, and 500 posters disseminated through the faith based organizations and universities, and Daily nation offered free advertisement. Since this is an annual event, the current study intends to examine its effectiveness on cybercrime awareness creation to the small business operators in Kasarani Sub-county Nairobi area.

2.3 Empirical Literature

From reviewed literature, it was quite clear that several scholars such as Kotuncu and Pusati (2019), Kang, Dabbish, Fruchter et al., (2015), Kumar et al. (2017), Weijer, Leckfeldt, and Zee (2021) among others observed that emerging technology has become more risk if the users fail to be aware about cybercrime prevention methods. They noted that an increase in innovations in different sectors of economy, has resulted to an increase in sophistication of cyber threats targeted to the users. However, they have all agreed that the users must be made aware about these cyber threats to avoid becoming victims.

In a research by Koyuncu and Pusati (2019) where they examined factors that influence a consumer before installing a mobile application in Europe concluded that consumers do not look more at security of device when determining risks. In other words, less risk leads to more trust, which then leads to an intention to install an application. They concluded that absence of information to the users is key to the growth of the cybercrimes and thus there is need to ensure that people are informed not to install applications that are not trusted. In order to install and use mobile device applications, a user is expected to first allow the application to access different resources such as his or her messages, photos among others, on his or her device. Despite these concerns, Koyunci and Pusati (2019), indicated that majority of the users tested in the study did not pay attention to this requirement, though it is expected by the application developer that the users are aware of what these applications can access, run, and activate on mobile phones. On the other hand, developers add mostly an end-user license agreement (EULA) document to inform and get consent from users about the application activities. However, this does not guarantee that the user reads and understands the content of EULA (Harris, Brookshire & Chin, 2016).

According to Koyuncu and Pusatli (2019), participants do not greatly recommend the use of the well develop security measures such as the EULAs, instead, they rely on the reuse of other applications that have been recommended by others based on their popularities and thus exposing their devices to the risk of being attacked in cybercrime related activities. On the other hand, developers cannot compel users to understand the content the agreement before consenting to the demands of the application. However, many users are not aware of the issues that they are agreeing on whenever they activate the user agreement. Hence, there is the need to ensure that there is assessment of the level of awareness that users have in terms of the issues that they agree on whenever they are installing applications.

In a review of literature, Kang, Dabbish, Fruchter et al., (2015) experimented on a mental model of Information Technology (IT) security for mobile devices. The study found out that users of mobile devices can be divided into two categories: those who consider their devices as a phone are associated with a lower security awareness and see themselves not responsible for the security of their devices; on the other hand, those who consider their devices as a smartphone are more aware of mobile security risks and also consider themselves more responsible to provide security for their devices. They advised further that, Information security is an issue for which multiple players such as the State, service providers, organizations, and individuals' should take responsibilities. Koyuncu and Pusatli (2019), observed that an attacker may deploy a rogue network access point, where he might intercept the user's communication, and carry out further attacks such as phishing.

Kumar et al. (2017) carried out a research on security awareness and cybercrime, and found out that an attacker might corrupt, block, or modify information on the wireless network by sniffing, spoofing, or eavesdropping. Furthermore, a malware in a smartphone can leak out information to unknown targets. Kumar et al. (2017), therefore, concluded that online presence increases risks for cyberattacks on mobile phone devices.

In reference to the current study, being unaware of risks of uncontrolled internet connections increase the chances for cyberattacks. This study therefore will seek to establish the level of awareness among the small business owners in Kasarani Sub-County. Koyuncu and Pusatli (2019), found out that the amount of personal data, sensitive documents, and credentials stored and processed by smartphones makes them an appealing target for attackers. Based on this fact that being aware of risks of storing credentials on smartphones is also selected as one of the parameters to be investigated to measure the security awareness level of smartphone users.

While focusing on malware targeting smart phones, Markelj and Bernik (2015) argued that when an application is installed on a mobile device, the user can only understand the use of the application based on the instructions provided by the application developer. Koyuncu and Pusatli (2019), further observed that the knowledge of threats that the users of mobile devices may face and the use of security measures are essential. In other words, users should be aware of security threats and mitigation measures. Based on this observations, the current study will establish the level of awareness of technical issues that are involved with smartphones. Other security related parameter such as password or pattern usage, application update behaviors of the users, pin usage will be included in this study.

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 (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 (Parker, Ophoff, Van Belle & Karia, 2015).

Zulkefli et al. (2017) study on the Typosquat Cyber Crime Attack Detection via Smartphone found out that a smartphone is either a medium of communication or a form of entertainment. Access to a smartphone owner, in exchange of information, by transmitting links or even files has become easier as a result of applications like SMS, Bluetooth, and services. Thus, viewed as an opportunity for any hacker to take advantage of hence leading to a great barrier in communication.

Kohar et al. (2015) studied the analysis of Smartphone users in United Sates of America, and how they created awareness on cyber phone crime activities. They found out that the relationship between crime rate and user awareness on cybercrime was significant. Kohar et al (2015) focused on characteristics of user such as level of awareness of smartphone users on cybercrime activity and what type of data the hacker targets. This study in relation to the current study is of much importance since it provides the rightful measures to handle the level of awareness of smartphone users against cybercrime activity. It also produces valuable research schemes. There are certain significant threats posed to smartphone users in relation to increased cybercrime cases.

Safavi et al. (2013) reviews on cybercrimes affecting portable observed that influx of different mobile phone products in the market has given its users a hard time in terms of securing their frames from potential data fissures. They argue that an increment in the number of exposures and attacks increases corresponds with the rise of security solutions offered by researchers. Safavi et al (2013) found out that most people using smartphones, and mobile portable devices, have heard about cybercrime on social media and television.

The permission-based security model and behavior-based detection have been suggested among the many few as defensive mechanisms for classified information.

According to Wright et al. (2012) a study on cybersecurity and mobile threats were done, and the importance of antivirus applications for smartphones was established, they found out that, 96% of smartphones lack pre-installed security software. This lack of security is open to malicious cyber attackers to hack into popular devices. They found out further that the usage of smartphones was high compared to personal computers when it came to handling personal tasks. Thus, making them more vulnerable.

Wright et al, (2012), reveals that smartphone users can perform several tasks using smartphones such as emailing, social networking via Facebook and Twitter, and other apps, purchasing and downloading several applications and shopping online. Moreover, monetary transactions can also be done whereby goods are bought, coupons and tickets redeemed, banking and processing point-of-sale payments. Financial transactions are eye-catching to cyber attackers since they only require to hack a user's smartphone, and get all information on anyone's bank account (Wright et al, 2012). Thus, this paper examines the importance of developing awareness among mobile phone users to protect their sensitive personal files.

The mass media according to Brown (2009), has been used in health promotion efforts for many years. She states further that television, newspapers, magazine, billboards and pamphlets have been used to encourage people to fasten seatbelts, and to use contraceptives among other uses. The current study intends to examine the role of KBA's initiative in creating public awareness about cybercrime prevention. This is in line with Brown (2009) argument that mass media can be effective in increasing awareness and stimulating attitude and behavior change among the audience. While supporting Brown

(2009) argument above, Chung (2018) observed that focused media coverage can have strong impact on public awareness and reaction to social issues by transmitting and sharing information about them.

The present study intends to highlight the extent to which small business operators who use smartphones in the study area have acquired information about how they should protect their devices against cybercrime. However, the current study will highlight previous studies that have focused on mass media coverage of different societal issues and draw parallels which would be helpful in the current study.

In a research carried out by Sampei and Aoyagi (2009), titled "Japanese newspaper coverage of global warming from January 1997 to July 2007 and how public opinion during that period was influenced by newspaper coverage," the results indicated that the growth of the coverage of the global warming in the newspaper was based on the public concern regarding the matter. In other words, some of the demands of the public can shape the discussions covered in the newspapers. This finding by Sampei and Aoyapi (2007) further imply that high level of media coverage let to effective communication of the climate change. Similarly, Mikami. Takeshika, and Kawabata (2011) in a related study, found out that reading a newspaper frequently was powerfully related with mobilization, and watching a lot of television had a weaker association of the same kind. Instead Newton (2010) observed that the media content rather than its form is what was important in creating awareness. The present study intends to examine how the KBA's content on cybercrime has impacted the perceptions of the small business owners' who rely on mobile phones to transact their businesses.

2.4 Conceptual Framework

The present study is guided by the conceptual framework that has been captured in figure 2.1. The conceptual framework shows the relationship between the independent and the dependent variable. In the conceptual framework, the independent variable is the cybercrime awareness and this is measured through assessing adoption of technology by small business users; extent to which small business operators understand about cybercrime prevention and the effectiveness of the KBA's initiative on cybercrime prevention. The dependent variable is the cybercrime prevention. The independent variables affect the dependent variable.

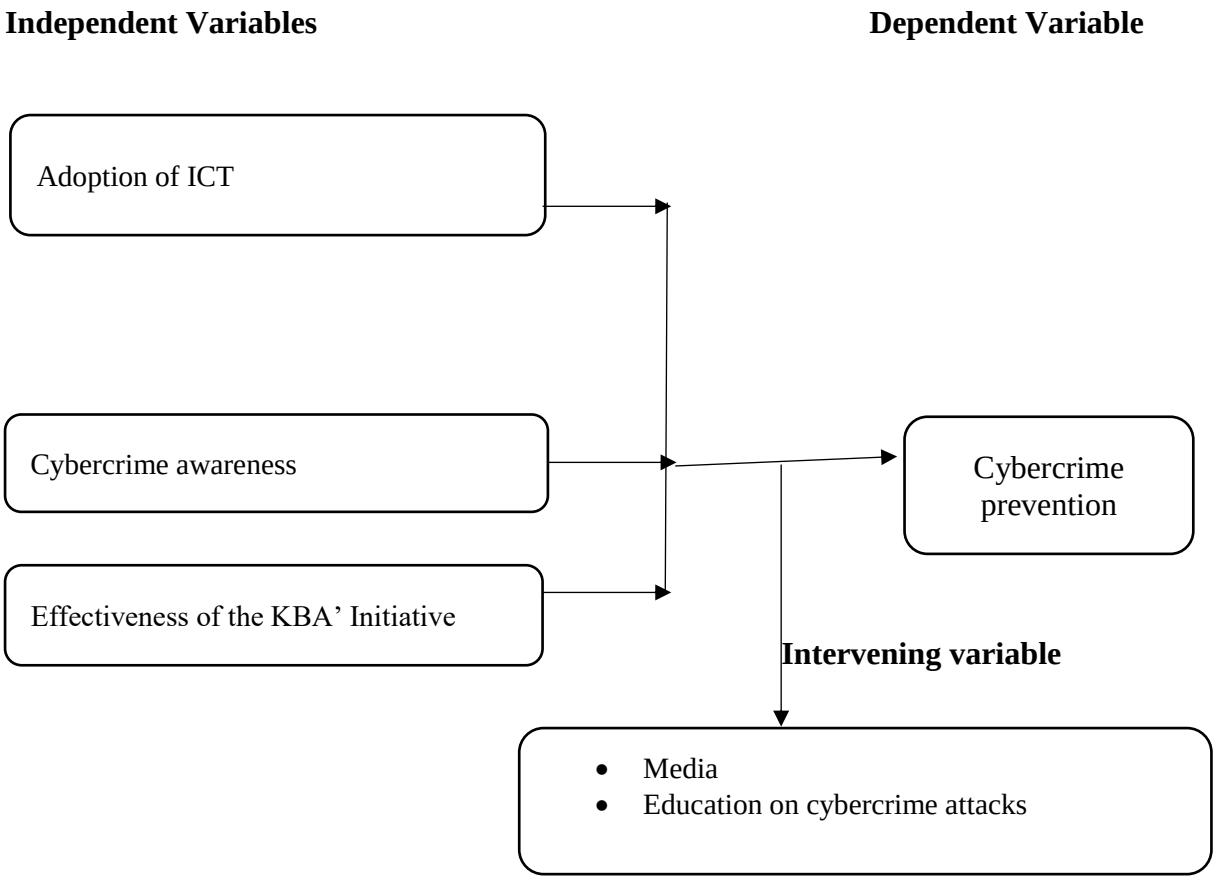

Figure 2.2: Conceptual Framework. Source: Author (2019).

2.5 Chapter Summary

The chapter covers various aspects as per the objectives of the research. The first aspect covered is about the theoretical framework that was used. The study used Diffusion of Innovation theory to examine how small business owners have adopted use of ICT in their operations. It was helpful in explaining how various small businesses have adopted the campaign messages by Kenya Bankers Association in preventing cybercrime attacks. The study also used Technology Acceptance Model (TAM), to explain factors that influence an individual to adopt the behavior that the campaign is pushing for.

The second issues captured is the general literature. The general literature highlights why cybercrime is a key problem world over. It is clear from the literature that many people in

Kenya access internet using their smartphones. On the other hand, we have empirical literature which is highlighting relevant studies which have been done that are related to this study. The next chapter will focus on the methodology of the study.

CHAPTER THREE

METHODOLOGY

3.0 Introduction

This chapter describes how the study was conducted, the research design that was used and target population considered in the study. Besides, the section highlights how respondents for the study was selected, the instrument used to collect data, ethical considerations, and concludes with the chapter summary.

3.1 Research Design

Survey research design was adopted in this study because it is suitable for collection of data from the sample population in order to determine status of that population in relation to one or more variables (Kothari, 2009). According to Mugenda and Mugenda (2003) this research design helps to denote the relationship between study variables, in this case the relationship between KBA's campaign strategies and public awareness about prevention of cybercrime. This study adopted ex-post facto design which is one of the survey research design because the small scale business owners under study have already been affected by the cybercrime issues and these could be studied retrospectively. This design was useful in collecting primary data that was used to examine the role of KBA's initiative in creation of public awareness.

3.2 Research Approach

This was a quantitative study since it sought to establish knowledge through use of numbers and measurements. Kothari (2004, p5) observed that quantitative research involves the generation of data in quantitative form which can be subjected to rigorous

quantitative analysis in a formal and rigid fashion. A structured questionnaire using predominantly closed ended questions was developed to collect data.

3.3 Study Area

The study was conducted at Kasarani Sub County. Kasarani is one of the constituencies in Nairobi County. The study area was selected because based on Kenya National Bureau of Statistics (KNBS) (2019), 2019 Kenya Population and Housing Census results, Kasarani Constituency was leading at the number of people from age 15 and above who access internet and bought items online at 15.4% followed by Embakasi constituency at 13.4%. In other words these are the people who have been affected by cybercrime in one way or another.

3.4 Population and Sampling

The target population of the study was mainly individuals who operate small businesses/transact online in Kasarani Constituency. In Kasarani Constituency there are a total of 79,594 people out of which 36,988 (13.4%) men, and 42602 (16.6%) are women (KNBS, 2019) operating small businesses. The small business do not employ more than five people in the case of this study.

3.5 Sampling Procedure

Kothari (2009) asserts that a sample is part of the target population that is used by the study. The researcher settled on a sample that best represents the target population. Sampling process is an activity that is done so as to settle on an appropriate number that can be used as a representative of the population that is being targeted (Kothari, 2009). The population was selected at 95% confidence level and 5% confidence interval.

3.5.1 Research Sample Size

The target adult population that is able to access internet in Kasarani Constituency according to 2019 Kenya Population and Housing Census Results is 79594. At the confidence level 95%, and confidence interval 5%, the study used a sample size of 398 respondents as indicated below:

$$n = \frac{N}{1+N\,(e)\,2}$$

In this formula, ***(n)*** is the sample size, ***(N)*** is the population size and ***(e)*** is the level of accuracy

$$n = \frac{79594}{1+79594\,(0.05 \times 0.05)} = \textbf{398} \text{ respondents}$$

A stratified random sampling was applied. According to Weaver, and Wilhoit (1990) it involved selection of sample from subset of a large population on the basis of specific probabilities calculated for each subset. The subsets in this study involved small business operators from various segments of economy in informal sector namely: Transport sector; juakali, shops, cybercafé, beauty shops, education sector among others. The simple random sampling according to Weaver, and Wilhoit (1990) involves selection of a small number of units from a larger set in such a way that all of the units in the larger set had an equal probability of being chosen. The sample was collected randomly from the following subset of small business owners: transport, M-pesa shops, Beauty shops groceries, security, education and others.

3.6 Data Collection Methods and Instruments

3.6.1 Development of Instruments

The researcher used primary data and secondary data. Primary data involved use of questionnaires that were designed based on the research questions in appendix I. The

questionnaire was structured in a manner that ensured that there was maximum collection of the intended information. The questionnaires were divided into two parts, that is the background information and another part for the research questions.

The first reason as to why the questionnaire was used is because it was time saving as it allowed for faster collection of data. The second reason for using questionnaires is that it is simple when it comes to testing the reliability and validity during the piloting stage. Thirdly, questionnaires allow for easier coding of the information that has been obtained through the use of any statistical tool that was used by the study (Mugenda, 2003).

3.6.2 Pilot Testing of Research Instruments

Pilot study was conducted within Ruiru Town, Kiambu County. The pilot study was used in the determination of the validity and reliability of the research. Ten (10) questionnaires were issued to small business operators to determine their validly and reliability. Views of respondents were to provide the required modification of the research instrument.

3.6.3 Instrument Validity

Validity is used to refer to the ability of the instrument to measure accurately what it is supposed to measure based on the content of application (Kombo & Tromp, 2006). Before the study was conducted, there was a pilot study that was conducted in order to determine the validly of the research instruments. The pilot study formed the basis for the improvement of the research instrument.

3.6.4 Instrument Reliability

Reliability is a measure of how the results from the test are consistent (Kombo & Tromp, 2006). Test-retest method was employed in determining the reliability of the research instrument.

3.7 Data Processing and Analysis

The data gathered was analyzed through the use of descriptive statistics. There was scrutiny of the questionnaires after the collection of the data before analysis was done in order to ensure that there was the cleaning of the information gathered prior to coding. The obtained data was coded into SPSS version 25.0 where results of the study were generation. All study variables were coded. Data was processed in order to generate the percentages and the frequencies of the findings. Analysis was done through interpretation of the findings that were obtained. Findings of the study were be conveyed through the use tables, charts and percentages to summarize the respondents' answers.

3.8 Ethical Considerations

Ethical aspects of the study were upheld through ensuring that there was confidentiality of the identity of the participants of the study as well as ensuring that integrity is applied when it comes to the results of the study.

An introduction letter from United States International University of Africa was obtained by the researcher and submitted to Nairobi County. A letter was attached to the questionnaire explaining the study to the respondents. Questionnaire were numbered so as to hide the identity of the participants.

The researcher obtained a permit from the Ministry of Science and Technology. The researcher also wrote a letter to the respondents explaining to them the study and asked for their consent to respond to the questionnaire.

3.9 Chapter Summary

The chapter describes the methodology and procedures that were used to carry out the study. It begun with an introduction underlining the general methodology and structure

of the chapter. The chapter also highlighted the method that was used to conduct the research and its justification. The population was defined, and the sampling technique, and sample size described. Finally, the data collection techniques and research procedures that was used have been discussed.

CHAPTER FOUR

FINDINGS AND ANALYSIS

4.1 Introduction

This chapter presents the results and findings of the study. The presentation is done as per the research questions/objectives. The results and findings are presented in form of tables and figures.

4.2 Response Rate

In this study, the researcher distributed 382 questionnaires, out of which 335 questionnaires were duly filled out and returned. The response rate of a test measures the statistical power of a research. A response rate of over 70% is acceptable; the higher the rate, the better. A total of 335 duly filled questionnaires out of 398 represents a response rate of 84.17%, which is acceptable, as shown in Table 4.1 below:

Table 4.1: Response rate

Questionnaires	Number	Percentage
Filled and collected	**335**	**84.17**
Non-Responded	**63**	**15.83**
Total	**398**	**100**

4.3 Reliability of the Study

Cronbach's alpha:

Table 4.2 shows that the reliability coefficient was found to be 0.855. The relationship between +/- 0.7 to 1.0 is strong. In this study, the Cronbach's Alpha was 0.855, which means the strength between features/variables influencing cybercrime prevention is very strong. Therefore, the disseminated questionnaire was strongly reliable for the study.

Table 4.2: Reliability of the Study

Reliability Statistics	
Cronbach's Alpha	N of Items
.855	12

4.4 Background Information of the Respondents

This section presents various socio-demographic attributes of the respondents in the study area. Such a profile is important in providing a basis for a clear understanding of the respondents included in the study and influences the results that shall follow based on the study's objectives.

4.4.1 Gender of Respondents

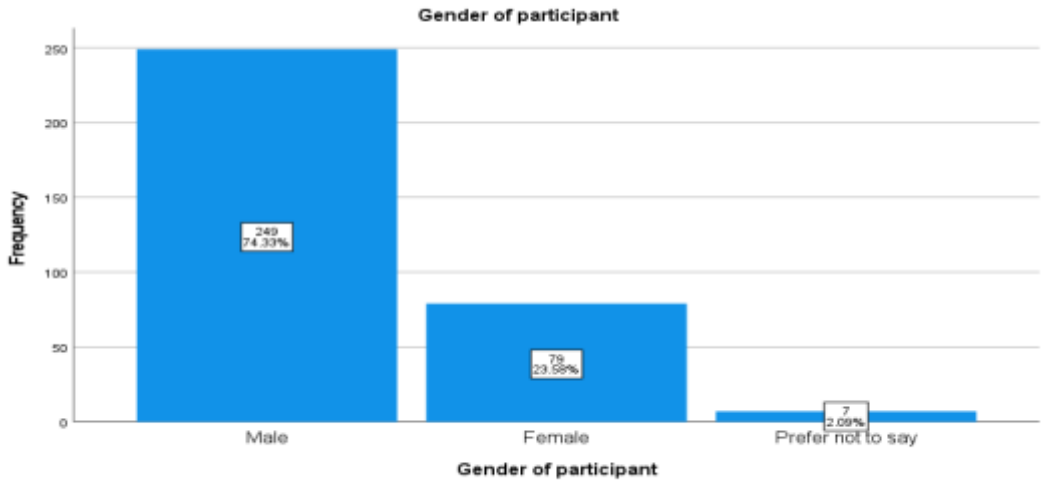

Figure 4.1: Gender of Respondent

The statistics on gender of respondents indicated that the majority were male (74%, n = 249), followed by females (24%, n= 79). The minority gender group consisted of 7 respondents who preferred not to say (2%, n= 7). These statistics are presented in figure 4.1 above.

4.4.2 Respondents Age Bracket

Respondents were asked to indicate their age bracket majority (144) were aged between 30-40 years (43%, N=335) followed by 120 respondents who indicated that they were aged between 18-30 years (36%, N=335), Minority were aged above 40 years (21%, N=335) as shown in figure 4.2 below.

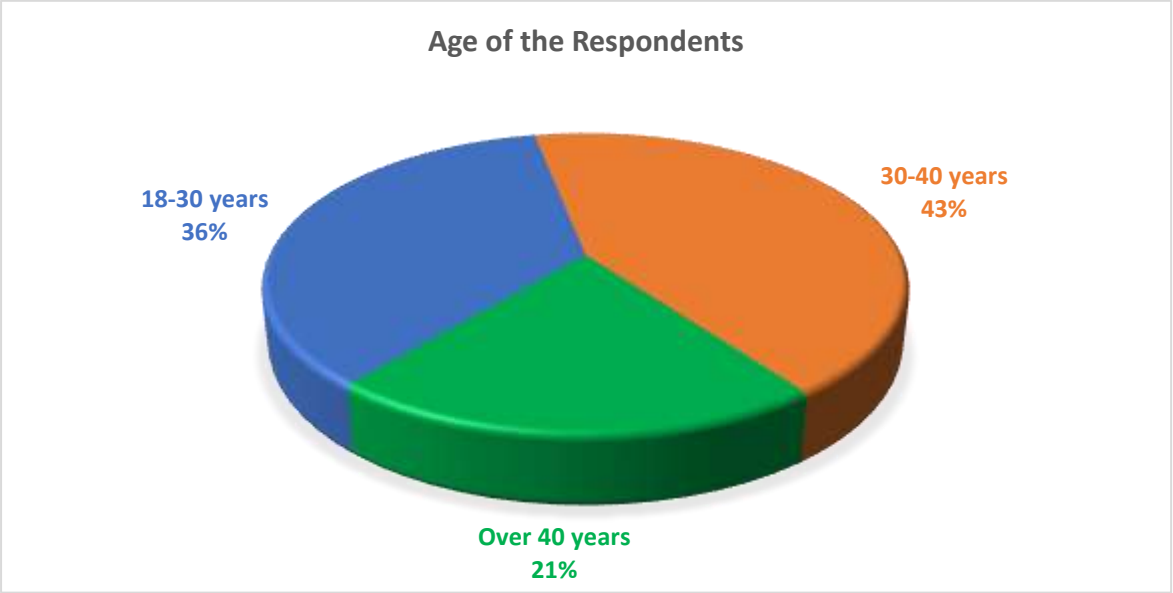

Figure 4.2: Respondents' Age Bracket

4.4.3 Highest Level of Education of Respondents

The study sought to establish the highest education level of the respondents. The findings indicated that most i.e. 180 respondents (54%, N = 335) had attained university level of education, followed by 65 respondents (19%, N = 335) indicated they had attained a college-level education, and 65 respondents (19%, N = 335) indicated that they had attained the secondary level of education. Minority of respondents (7.5%, N = 335) indicated that they had only attained the primary level of education. These statistics are shown in figure 4.3 below.

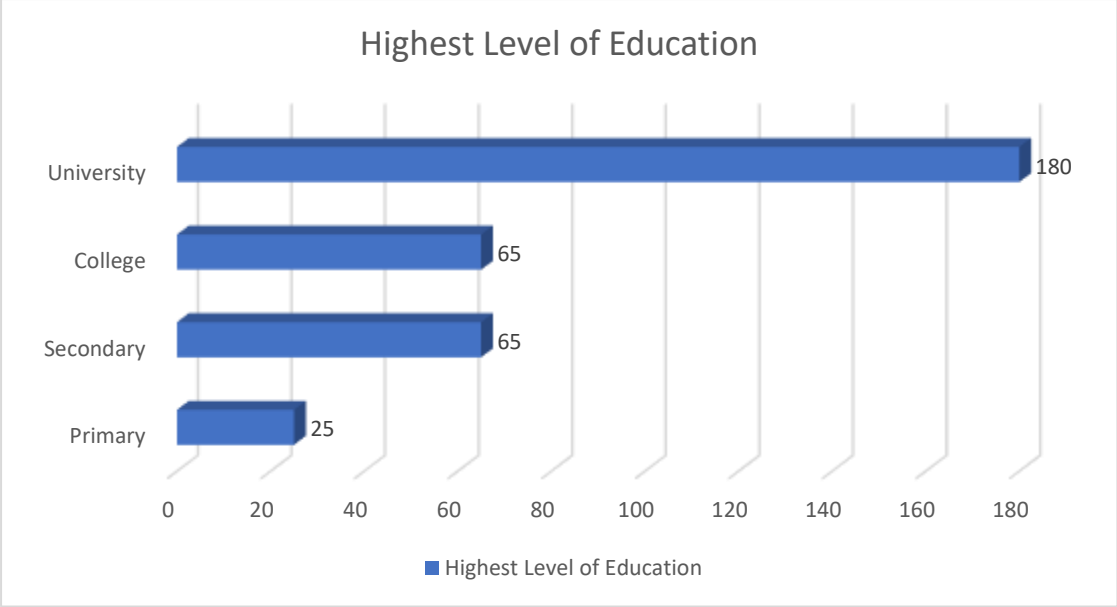

Figure 4.3: Highest Level of Education

4.4.4 Length Respondent has operated their Business in the Kasarani Constituency

Respondents were asked to indicate the duration that they had operated their business.

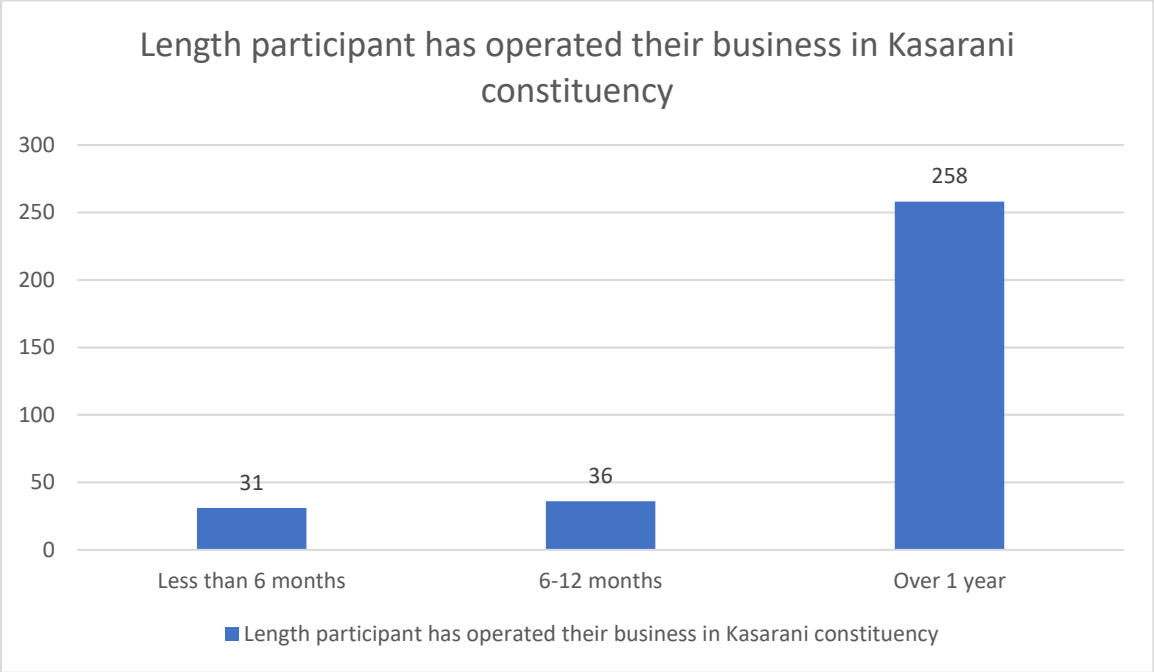

Figure 4.4: Length Respondents has operated their business in the Kasarani constituency

The findings in figure 4.4 above showed that the majority, 258 of the respondents (77%, N = 335) had operated their business for over 1 year, followed by 36 respondents (10.7%, N = 335) who indicated that they have operated their business in Kasarani area for

between 6 and 12 months. The minority group comprised 31 respondents (9.3%, N = 335) who had operated their business for less than 6 months.

4.4.5 Training on Computer-related Threats and Crime

The study sought to establish whether respondents had been trained on computer-related threats and crime. The statistics showed that 135 respondents (40%, N=335) had been trained on computer-related threats and crime. In comparison majority, 200 participants (60%, N=335) indicated that they had not been trained on computer-related threats and crime. These statistics are shown in figure 4.5 below.

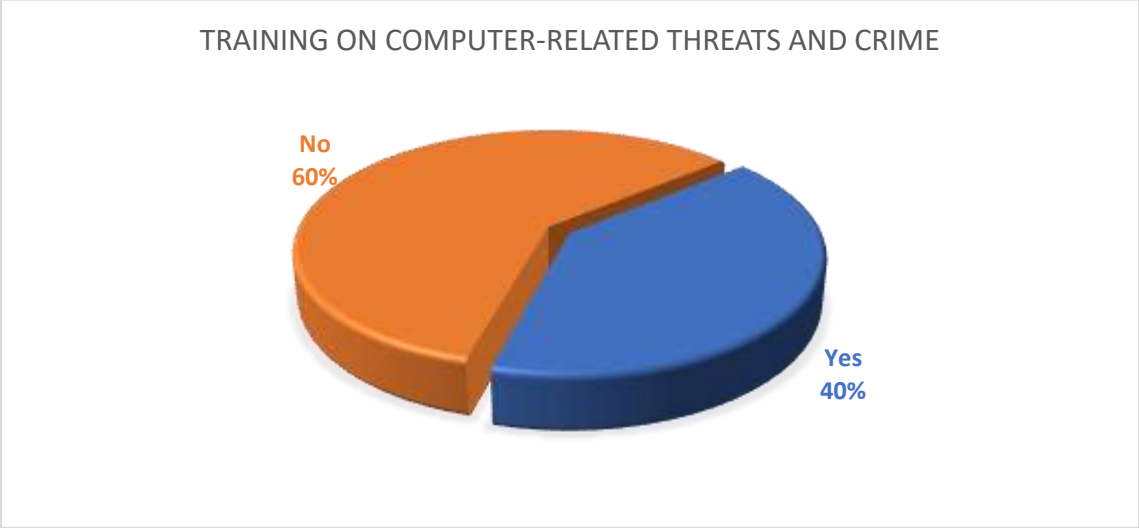

Figure 4. 5: Trained On Computer-Related Threats And Crime

4.5 Research Objective 1: How Small Business Operators in the Kasarani sub-County have adopted the use of ICT in their Businesses

One of the study's research objectives was to examine how small business operators in Kasarani sub-county had adopted ICT in their businesses. The following are the findings:

4.5.1 Small Businesses Respondents are Operating

Respondents involved in the study were operating a wide range of small businesses. The most common businesses were: the transport sector, Mpesa shops, beauty shops, groceries, security, education sector, and other shops.

4.5.2 Mobile Phone usage in Small Businesses

Respondents were asked if they used their mobile phones in their businesses. The findings showed that majority 314 respondents (93.7%, n= 314) indicated that they used mobile phones in their small businesses. In comparison, 21 respondents (6.3%, n=21) indicated that they do nto use their mobile devices in their business. This is as shown in figure 4.6 below:

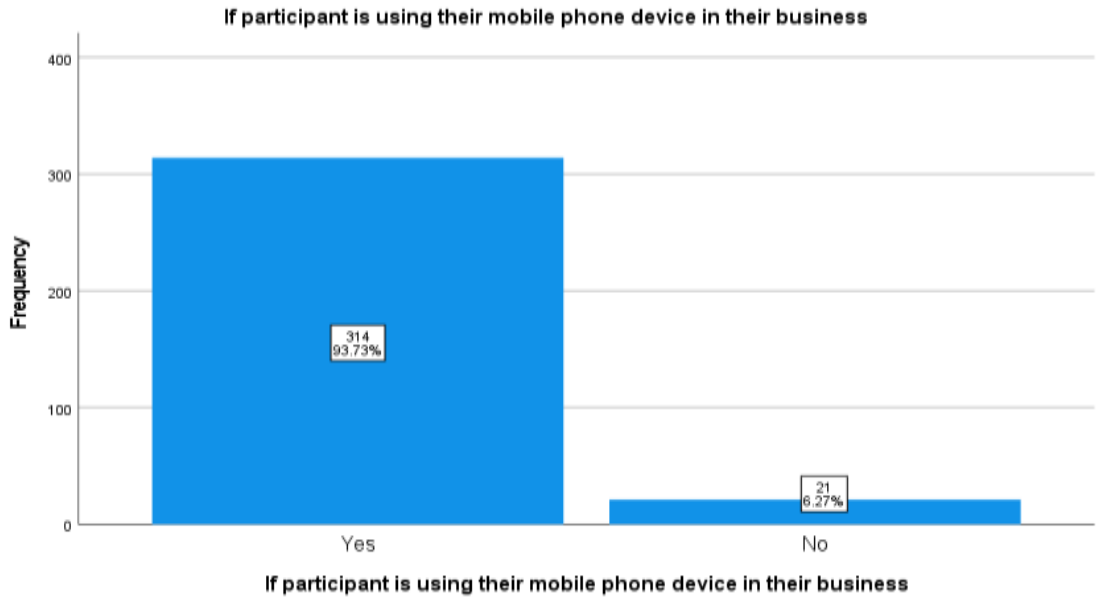

Figure 4.6: Mobile Phone Usage In Small Businesses

4.5.3 Purpose of the Mobile Phone in Businesses

The study sought to establish the purpose of using a mobile phone in businesses. The findings showed that 308 of the 335 respondents use their mobile phones to socialize; 285 of the 335 respondents use their mobile phones for banking; 268 of the 335 respondents use their mobile phones in shopping; 263 of the 335 respondents used their mobile phones to check and reply to emails; 242 of the 335 respondents use their mobile phones in research; 210 of the 335 respondents use their mobile phones to download music and movies, and 63 of the 335 respondents use their mobile phones to gamble. The minority, 26 of the 335 respondents, use their mobile phones in auctioning. These statistics are presented in figure 4.7 below:

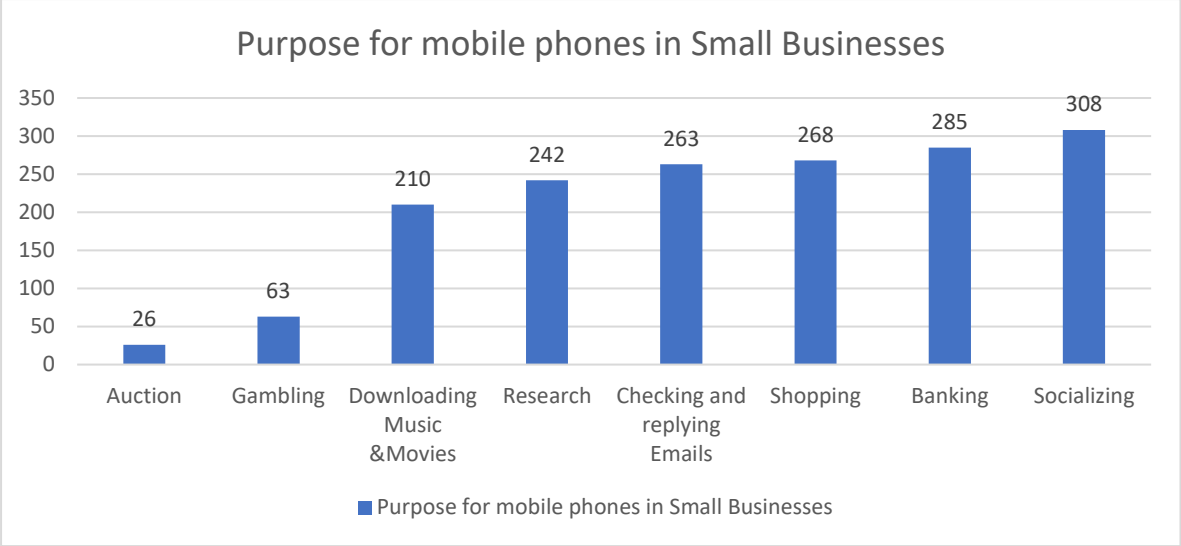

Figure 4.7: Purpose of the Mobile Phone in Businesses

4.5.4 Factors that influenced the use of Mobile Phone Technology in Operations/Businesses

Respondents were asked to indicate the factor(s) that influenced them to use mobile phone technology in their operations/businesses. The following are the most common factors highlighted.

i. Communication

Respondents highlighted that they use phones for easier communication, reach out to customers and potential customers, and timely engagements

ii. Convenience

Respondents also highlighted the convenience that comes with having a mobile phone; flexibility, proximity, internet connectivity, cost, convenience

iii. Online Businesses and advertising their products or services

Respondents indicated that they advertise their products and services online for them to get customers. Example that was given is that they take pictures over their phones which they share with potential customers through various social media platforms online. The small business owners in the transport sectors use various mobile hail-riding services to access their customers.

iv. Socializing

They socialize with their potential customers and get to display their products and services through socialization.

v. Mobile money transactions

Majority use the mobile money services to carry out transactions.

vi. Covid-19 pandemic

They cited government regulation on use of mobile money transfers services as a measure of mitigating covid-19 pandemic.

vii. Real-time news

Respondents indicated that through the online platforms, they get really time news concerning their products and services.

viii. Listening to music and watching movies

They download and listen to music online while contacting their various businesses.

ix. Linking with other businesses and technologies

Respondents indicated that through various platforms online, they get in touch with other businesses interested in their or vice versa.

4.6 Objective 2: To assess cybercrime awareness among the small business operators in Kasarani sub-county, Nairobi.

4.6.1 Cybercrime Incidences Experienced

The study sought to establish the type of cybercrime incidences experienced by the respondents. The statistics showed that majority (91% =335) experienced hacking; 84 of the 335 respondents experienced data theft, 82 of the 335 respondents experienced denial of service; and 62 of the 335 respondents experienced identity theft. This is as shown in figure 4.8 below:

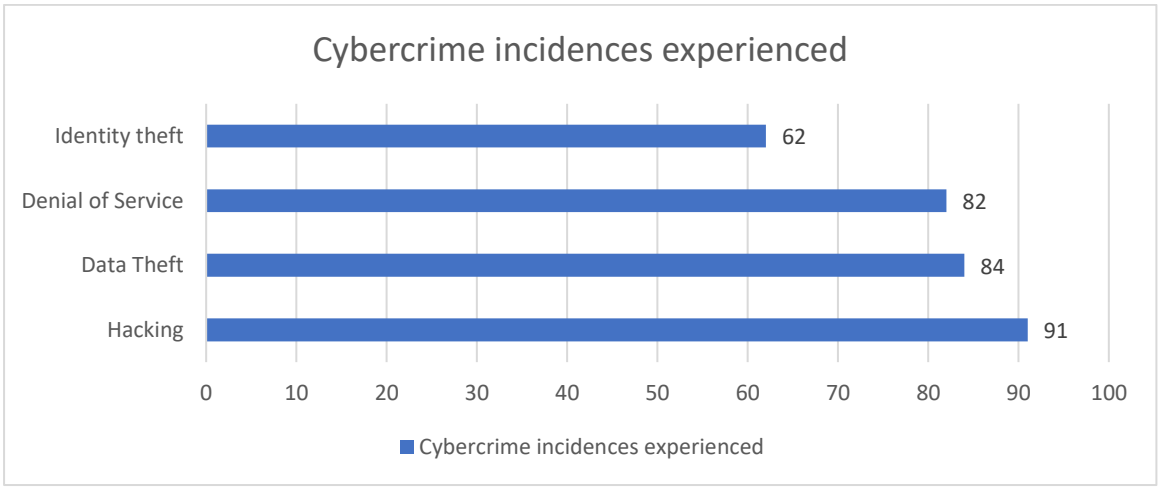

Figure 4.8: Cybercrime incidences experienced

4.6.2 Awareness of Cybercrime Issues

Respondents were asked questions regarding their awareness about cybercrime. Responses were captured in a Linkert scale with the coding; 5 -Strongly Agree, 4 -Agree, 3 -Undecided, 2 - Disagree, 1 -Strongly Disagree. Frequency percentages (Most selected response), means, and standard deviations (SD) were the main tools of Analysis for the measurement of this construct, as shown below.

Table 4.3: Awareness of Cybercrime Issues

Awareness about Cybercrime Variables	1 (%)	2 (%)	3 (%)	4 (%)	5 (%)	Mean	SD
I only install a mobile applications that are trusted over my phone	14.9	13.4	6.0	38.5	24.5	**3.45**	**1.398**
Before installing an application, I usually read the application provider's privacy and policy for using the application	24.8	23.3	11.3	23.9	12.8	**2.76**	**1.415**
I usually store most of my credential/documents over my phone	24.8	31.3	7.8	24.5	9.6	**2.62**	**1.354**
I usually use free Wi-Fi whenever I access it	24.5	23.9	8.1	21.5	19.7	**2.88**	**1.506**

From to table 4.3 above, most respondents agreed that they only install mobile applications that are trusted over their phone (Percentage = 38.5, Mean = 3.45, Standard Deviation = 1.398). Most respondents strongly disagreed that they usually read the application provider's privacy and policy for using the application before installing the application (Percentage = 24.8, Mean = 2.76, Standard Deviation = 1.415). Most study participants strongly disagreed that they usually store most of their credentials/documents over their phone (Percentage = 24.8, Mean = 2.62, Standard Deviation = 1.354). Most

respondents strongly disagreed that they usually use free Wi-Fi whenever they access it (Percentage = 24.5, Mean = 2.88, Standard Deviation = 1.506).

4.7 Research Objective 3: To assess the perception of the small business operators on effectiveness of Strategies employed by the Kenya Bankers Association initiative "Kaa Chonjo" in curbing cybercrime

The third objective of the study was to assess the perception of small business operators on effectiveness of the Kenya Bankers Association initiative "Kaa Chonjo" on curbing cybercrime. This was analyzed through descriptive and inferential statistics (Correlation, Regression, and ANOVA) to test the strength of the relationship and the effect of the Kenya Bankers Association Campaign on curbing cybercrime.

4.7.1 Descriptive statistics; Kenya Bankers Association Campaign

Respondents were asked questions regarding Kenya Bankers Association Campaign. Table 4.4 below presents responses to statements regarding Kenya Bankers Association Campaign:

Table 4.4: Kenya Bankers Association Campaign

Kenya Bankers Association Campaign Strategies	1 (%)	2 (%)	3 (%)	4 (%)	5 (%)	Mean	SD
I heard cybercrime prevention strategy dubbed "Kaa Chonjo" through the mass media (Radio, Television, and Newspaper)	14.3	17.6	6.0	40.0	19.1	**3.33**	**1.367**
I got the information on cybercrime prevention through Information, Education, and communication material (IEC) distributed to me by the Kenya Bankers association/associates	23.6	43.6	7.5	15.5	6.9	**2.37**	**1.211**
I learned about cybercrime prevention through pamphlets distributed by the Kenya Association of Bankers	30.4	46.6	7.8	8.7	3.3	**2.05**	**1.029**
I learned about cybercrime prevention through the formal campaign initiative by Kenya Bankers Association that I have participated in	35.2	41.8	6.0	9.6	3.9	**2.02**	**1.091**

The findings indicate that the majority of the participants agreed that they heard cybercrime prevention strategy dubbed "Kaa Chonjo" through the mass media (Radio, Television, and Newspaper – Percentage = 40.0, Mean = 3.33, Standard Deviation = 1.367). Most respondents disagreed that they got the information on cybercrime prevention through Information, Education, and communication (IEC) material distributed to them by the Kenya Bankers association/associates (Percentage = 43.6, Mean = 2.37, Standard Deviation = 1.211). Most study participants disagreed that they learned about cybercrime prevention through pamphlets distributed by the Kenya Association of Bankers (Percentage = 46.6, Mean = 2.05, Standard Deviation = 1.029). Most respondents disagreed that they learned

about cybercrime prevention through the formal campaign initiative by Kenya Bankers Association they have participated in (Percentage = 41.8, Mean = 2.02, Standard Deviation = 1.091).

4.7.2 Correlation Analysis: Correlation between Cybercrime awareness level and Kenya Bankers Association campaign ("Be alert," / "Kaa Chonjo" strategy)

A correlation test was done to investigate the significant relationship between the Kenya Bankers Association campaign and cybercrime awareness. The results indicated a positive, relatively strong relationship between the Kenya Bankers Association initiative and cybercrime awareness (r=0.397, p=<0.001), as shown in Table 4.5 below. This implied that an increase in the Kenya Bankers Association campaign ("Be alert," / "Kaa Chonjo" strategy) leads to increased cybercrime awareness hence curbing cybercrime.

Table 4.5: Correlation between Cybercrime awareness level and Kenya Bankers Association campaign

Correlations			
		Kenya Bankers Association Campaign	Cybercrime Awareness
Kenya Bankers Association Campaign	Pearson Correlation	1	.397**
	Sig. (2-tailed)		<.001
	N	314	303
Cybercrime Awareness	Pearson Correlation	.397**	1
	Sig. (2-tailed)	<.001	
	N	303	315

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

4.7.3 Regression Analysis: Effect of Kenya Bankers Association campaign ("Be alert," / "Kaa Chonjo" strategy) on Cybercrime awareness level.

Table 4.6: Regression Analysis; Kenya Bankers Association campaign versus Cybercrime awareness level

Model Summary				
Model	**R**	**R Square**	**Adjusted R Square**	**Std. Error of the Estimate**
1	**.397[a]**	**.157**	**.155**	**.88085**

a. Predictors: (Constant), Kenya Bankers Association Campaign

Table 4.6 above shows that the coefficient of determination also called the R square, is 0.157. This means that the combined effect of the predictor/independent variable (i.e., the Kenya Bankers Association campaign) explains approximately 15.7% of the variations in cybercrime awareness. The correlation coefficient of 0.397 indicates that the combined effect of the predictor variables (Kenya Bankers Association campaign) has a relatively strong positive correlation versus cybercrime awareness.

4.7.4 Analysis of Variance (ANOVA); Kenya Bankers Association campaign versus Cybercrime awareness level.

Table 4.7: Analysis of Variance (ANOVA); Kenya Bankers Association campaign versus Cybercrime awareness level

Anova

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	43.621	1	43.621	56.221	<.001[b]
	Residual	233.543	301	.776		
	Total	277.164	302			

a. Dependent Variable: Cybercrime Awareness

b. Predictors: (Constant), Kenya Bankers Association Campaign

Table 4.7 above shows the Analysis of variance (ANOVA). The findings showed that the combined effect of variables on the Kenya Bankers Association campaign was statistically significant in explaining changes in cybercrime awareness. This is demonstrated by a p-value of less than 0.001, which is less than the critical acceptance value of 0.05.

4.8 Intervening Variable Analysis – Media Strategies Impact on Kenya Bankers Association campaign and Cybercrime Awareness

The intervening variable (Media Strategies) explains the cause or connection between the Kenya Bankers Association initiative and cybercrime awareness. The intervening variable hypothetically links the Kenya Bankers Association initiative and cybercrime awareness. The analysis included the descriptive Analysis of the statements on

media strategies and the inferential statistics between media strategies, the Kenya Bankers Association initiative, and cybercrime awareness.

4.8.1 Descriptive Statistics; Media Strategies

Respondents were asked questions regarding media strategies. Responses were captured in a Linkert scale with the coding; 5 -Strongly Agree, 4 -Agree, 3 -Undecided, 2 - Disagree, 1 -Strongly Disagree. Frequency percentages (Most selected response), means, and standard deviations (SD) were the main tools of Analysis for the measurement of this construct, as shown below.

Table 4.8: Descriptive Statistics; Media Strategies

Media Strategies	1 (%)	2 (%)	3 (%)	4 (%)	5 (%)	Mean	SD
The media has informed me of the tricks that are used by criminals involved in cybercrime	9	11	6.6	51	21.2	**3.65**	**1.195**
The media has informed me on the measures to take to avoid cases of cybercrime within my business	10.7	11.9	5.4	52.8	17.3	**3.55**	**1.227**
The media has made me know steps to take to prevent a cyberattack on my internet device	10.4	16.4	11.9	44.2	13.7	**3.35**	**1.227**
Since being informed by the media about cybercrime, I have not been a victim	10.4	14.0	8.1	51.9	12.8	**3.44**	**1.203**

Table 4.8 presents responses to statements regarding media strategies. The findings showed that most of the participants agreed that the media had informed them of the tricks used by criminals involved in cybercrime (Percentage = 51, Mean = 3.65, Standard

Deviation = 1.195). Most respondents agreed that the media had informed them of the measures to avoid cybercrime within their business (Percentage = 52.8, Mean = 3.55, Standard Deviation = 1.227). Most study participants agreed that the media had made them know steps to take to prevent a cyberattack on their internet device (Percentage = 44.2, Mean = 3.35, Standard Deviation = 1.227). Most respondents agreed that since being informed by the media about cybercrime, they had not been a victim (Percentage = 51.9, Mean = 3.44, Standard Deviation = 1.203).

4.8.2 Impact of media strategies on the Kenya Bankers Association campaign

Theoretically, the intervening variable impacts the dependent and independent variables (the Kenya Bankers Association campaign and cybercrime awareness). Inferential Analysis is therefore needed to test the association between media strategies, the Kenya Bankers Association campaign, and cybercrime awareness.

4.8.2.1 Correlation Analysis: Correlation between Media strategies and Kenya Bankers Association campaign ("Be alert," / "Kaa Chonjo" strategy)

A correlation test was conducted to investigate the relationship between the Kenya Bankers Association campaign and media strategies. The results indicated a positive, strong relationship between media strategies and the Kenya Bankers Association initiative (r=0.480, p=<0.001), as shown in Table 4.9 below. This implied that media strategies had a strong direct influence on the Kenya Bankers Association Campaign.

Table 4.9: Kenya Bankers Association initiative vs. cybercrime awareness

Correlations

		Media strategies impact	Kenya Bankers Association Campaign
Media strategies impact	Pearson Correlation	1	.480**
	Sig. (2-tailed)		<.001
	N	322	308
Kenya Bankers Association Campaign	Pearson Correlation	.480**	1
	Sig. (2-tailed)	<.001	
	N	308	314

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

4.8.2.2 Regression Analysis: Effect of Media Strategies on Kenya Bankers Association campaign ("Be alert," / "Kaa Chonjo" strategy).

Table 4.10: Regression Analysis: Media Strategies versus Kenya Bankers Association campaign

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.480[a]	.231	.228	.79550

a. Predictors: (Constant), Media strategies impact

Table 4.10 above shows that the coefficient of determination also called the R square, is 0.231. This means that the combined effect of the intervening variable (i.e., media strategies) explains approximately 23.1% of the Kenya Bankers Association campaign variations. The correlation coefficient of 0.480 indicates that the combined effect of the mediating variable (impact of media strategies) has a strong positive correlation versus the Kenya Bankers Association campaign.

4.8.2.3 Analysis of Variance (ANOVA): Media strategies impact versus Kenya Bankers Association campaign.

Table 4.11: ANOVA; Media strategies impact versus Kenya Bankers Association campaign

ANOVA

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	58.044	1	58.044	91.723	<.001[b]
	Residual	193.643	306	.633		
	Total	251.687	307			

a. Dependent Variable: Kenya Bankers Association Campaign

b. Predictors: (Constant), Media strategies impact

Table 4.11 above shows the Analysis of variance (ANOVA). The findings showed that the combined effect of variables on media strategies was statistically significant in explaining changes in the Kenya Bankers Association initiative. This is demonstrated by a p-value of less than 0.001, which is less than the critical acceptance value of 0.05**.**

4.8.3 Impact of media strategies on cybercrime awareness

4.8.3.1 Correlation Analysis: Correlation between Media strategies and cybercrime awareness.

A correlation test was conducted to investigate the relationship between media strategies and cybercrime awareness. The results indicated a positive, strong relationship between media strategies' impact and cybercrime awareness (r=0.456, p=<0.001), as shown in Table 4.12 below. This implied that media strategies had a strong direct influence on cybercrime awareness.

Table 4.12: Correlation Analysis; Media strategies versus cybercrime awareness

Correlations

		Media strategies impact	Cybercrime Awareness
Media strategies impact	Pearson Correlation	1	.456**
	Sig. (2-tailed)		<.001
	N	322	307
Cybercrime Awareness	Pearson Correlation	.456**	1
	Sig. (2-tailed)	<.001	
	N	307	315

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

4.8.3.2 Regression Analysis: Effect of Media Strategies on cybercrime awareness

Table 4.13: Regression Analysis; Media strategies versus cybercrime awareness

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.456[a]	.208	.205	.85342

a. Predictors: (Constant), Media strategies impact

Table 4.13 above shows that the coefficient of determination also called the R square, is 0.208. This means that the combined effect of the intervening variable (i.e., media strategies explains approximately 20.8% of the variations in cybercrime awareness. The correlation coefficient of 0.456 indicates that the combined effect of the mediating variable (impact of media strategies) has a strong positive correlation versus cybercrime awareness.

4.8.3.3 Analysis of Variance (ANOVA); Media strategies impact versus cybercrime awareness.

Table 4.14: Analysis of Variance (ANOVA); Media strategies impact versus cybercrime awareness.

ANOVA

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	58.241	1	58.241	79.964	<.001[b]
	Residual	222.142	305	.728		
	Total	280.383	306			

a. Dependent Variable: Cybercrime Awareness

b. Predictors: (Constant), Media strategies impact

Table 4.14 above shows the Analysis of variance (ANOVA). The findings showed that the combined effect of variables on media strategies was statistically significant in explaining changes in cybercrime awareness. This is demonstrated by a p-value of less than 0.001, which is less than the critical acceptance value of 0.05

4.9 Chapter Summary

The chapter presented the results of major findings of the research based on three research objectives, namely how small business operators in Kasarani sub-county have adopted the use of ICT in their businesses, cybercrime awareness among the small business operators in the Kasarani sub-county, Nairobi and the effectiveness of strategies employed by the Kenya Bankers Association initiative "Kaa Chonjo" in curbing cybercrime. The chapter also presented the findings on the effect of media as an intervening variable on the Kenya Bankers Association initiative and cybercrime awareness. The next chapter presents discussions, conclusions, and recommendations.

CHAPTER FIVE

DISCUSSIONS, CONCLUSIONS, AND RECOMMENDATIONS

5.1 Introduction

This chapter is divided into three sections: discussions, conclusions, and recommendations. It presents the results' ramifications, linking them to the literature, and offers empirically supported conclusions and suggestions for action. Additionally, this chapter offers suggestions for additional research based on the findings, research flaws, suggested investigations, and development of the framing theory.

The study on the effectiveness of online safety awareness campaign strategies by the Kenya Bankers Association sought to examine how small business operators in the Kasarani sub-county have adopted the use of ICT in their businesses, assess the extent of cybercrime awareness among the small business operators in Kasarani, and assess the effectiveness of strategies employed by the Kenya Bankers associations initiative 'kaa chonjo' in curbing cybercrime.

5.2 Summary of Findings

The analysis of gender rating indicates that the majority (74%) of the small business operators in Kasarani Sub-county are males compared to 24% percent of females, two (2) percent of the study respondents preferred not to disclose their gender. Most small business operators are also aged between 30-40 years (43%), followed by those aged between 18-30 years (36%), and 21% indicated that they were over 40 years. At the education level, the majority (54%) of the small business operators were university graduates, followed by college and secondary education with 19% representation. The minority group comprised approximately 8% of respondents who indicated that primary school was their highest level of education. The findings on training on computer-related threats and crime showed that 60% of the respondents had not been trained, and 40% agreed to have been trained on computer-related threats and crime.

The outcomes on the adoption of mobile phone devices in operating small businesses indicated that the small businesses in the study areas range from beauty shops,

education, mpesa shops, general shops, transport, security, sales and supplies, and selling farm produce and others. The operators of these businesses use the mobile phone for the following purposes: Socializing, checking and replying to emails, researching for new products, shopping, searching for the information, downloading music and movies, gambling, banking, and auction. The outcome of the above objective indicates that these businesses have majorly adopted mobile phones because of their convenience for business operations and easier communication between them and their customers. Other reasons advanced for adopting mobile phone devices in businesses include using mobile money services such as mpesa (mobile money transactions) and advertising their products.

The second objective which was to assess cybercrime awareness among the small business operators in Kasarani sub-county, Nairobi, findings indicates most of the small business operators have been hacked, other have experienced data theft, denial of services, and identity theft. This can be attributed to the previous finding that only 40 percent of the respondents had been trained on cybercrime prevention. The study findings indicates that most participants only install mobile applications that are trusted over their phone (Percentage = 38.5, Mean = 3.45, Standard Deviation = 1.398). Most respondents strongly disagreed that they usually read the application provider's privacy and policy for using the application before installing the application (Percentage = 24.8, Mean = 2.76, Standard Deviation = 1.415). Most study participants strongly disagreed that they usually store most of my credentials/documents over their phone (Percentage = 24.8, Mean = 2.62, Standard Deviation = 1.354). Most respondents strongly disagreed that they usually use free Wi-Fi whenever I access it (Percentage = 24.5, Mean = 2.88, Standard Deviation = 1.506).

The summary findings on the third objective; to assess the perception of the small business operators' on effectiveness of strategies employed by the Kenya Bankers Association initiative "Kaa Chonjo" in curbing cybercrime, showed that the majority of the respondents heard cybercrime prevention strategy dubbed "Kaa Chonjo" through the mass media (Radio, Television, and Newspaper). Inferential statistics were done to test the strength of the relationship between KBA strategies and cybercrime awareness and how effective it is in curbing cybercrime. The strength of the relationship showed a positive, relatively strong relationship between the Kenya Bankers Association initiative and cybercrime awareness ($r=0.397$, $p=<0.001$). The linear regression analysis to test how effective the KBA initiative was revealed that the KBA strategies explained 15.7% of the

variability in the cybercrime awareness. One Way ANOVA test results showed a statistically significant difference in the effect of the KBA initiative on cybercrime awareness.

5.3 Discussion

The study's findings in light of the research questions are discussed in this section. Each study question's significant findings are explained in relation to the literature review.

5.3.1. Extent to which small business operators have adopted use of ICT in their businesses

The study findings from the descriptive analysis reveals that most of the respondents were using mobile phones to operate their small businesses. Most small businesses were beauty shops, learning institutions, M-pesa shops, general shops, transport, security, sales and supplies, farm produce, and others. These findings are consistent with (Awinja & Fatoki, 2021), who found that most SMEs within Nairobi County, Kenya is in security, transport, shops, etc. This may be because most of these small businesses need less capital to start.

The outcome of the above objective indicates that these businesses have majorly adopted mobile phones because of their convenience for business operations and easier communication between them and their customers. Other reasons advanced for adopting mobile phone devices in businesses include using mobile money services such as mpesa (mobile money transactions) and advertising their products. The results are also consistent with (Masood & Sonntag, 2020), who found out that it is easy to set up small businesses due to their flexibility, cost, efficiency, quality, and competitive advantage benefits

5.3.2. Assessing cybercrime awareness level among the small business operators in Kasarani sub-county, Nairobi

The findings on the second objective indicated that most participants agreed that they only install mobile applications that are trusted over their phone. These findings were in agreement with (Chin et al., 2018), who found out that most mobile users install applications from genuine application stores (e.g., google and apple stores).

Most respondents strongly disagreed that they usually read the application provider's privacy and policy for using the application before installing the application. According to (Meier et al., 2020), most technology users ignore the provider's privacy and policy since they are mostly lengthy and hence an insufficient number of users read them to completion. As a result of this, the small business operators in Kasarani Sub-county have experienced cybercrime such as hacking, data theft, denial of services and identity theft. This is because they have installed applications on their mobile phones that are able to access their different resources such as the messages, personal data and documents among others in the process compromising the security of their information. It is important to note that lack of information to the small business operators is key to the growth of cybercrimes, and thus there is need to ensure that small business operators are informed not to install mobile phone applications that are not trusted.

The study found out that most of the small business operators do not store their data on their mobile phone devices, and that they do not use free wifi. This is key in prevention of cybercrime attacks. However, more than 60% of the small business operators in study area stated that they have not been trained on cybercrime prevention. This implies therefore that they either have no documents to store on their devices, and or free wi-fi connections are not readily available to test whether they are taking these precautions out of knowledge or by chance.

5.3.3. To assess the perception of the small business operators on effectiveness of strategies employed by the Kenya Bankers Association initiative "Kaa Chonjo" in curbing cybercrime.

The findings on the relationship's strength showed a positive, relatively strong relationship between the Kenya Bankers Association initiative and cybercrime awareness. According to (Mbogo, 2018), KBA initiative aimed to increase awareness on a larger scale to help curb cybercrime. The linear regression results showed that the Kenya Bankers Association initiative directly influenced cybercrime awareness. It revealed that the KBA strategies explained 15.7% of the variability in cybercrime awareness.

The study found out that most effective KBA’s strategy on preventing cybercrime on small business operators was through the mass media specifically Radio, Television, and

newspapers. However, other forms of information sharing such as distribution of Information Education and Communication (IEC) materials, pamphlets, and formal campaign strategies by KBA was not effective, as mass media. This implies that KBA should use mass media platforms-radio, Television and Newspapers in their cybercrime campaigns more as opposed to other strategies of campaign.

They should also carry out the baseline survey to establish the needs of various small businesses online and offer targeted information or training that will enable the target groups of small business operators to be prevent cybercrime attacks.

5.4 Conclusions

The discussion of the key findings led to the following conclusions.

5.4.1 How small business operators have adopted use of ICT in their businesses

The study revealed that small business operators in Kasarani have adopted ICT in their businesses. This was majorly through the use of mobile phones in many business operations, e.g., sales and money transfers. This implies that most small business operators have adopted ICT use in their operations to offer their products and services better. It can be concluded that ICT has been adopted largely by small business operators in their day-to-day activities

5.4.2 Assessing cybercrime awareness level among the small business operators in Kasarani sub-county, Nairobi

In assessing cybercrime awareness among the small business operators in Kasarani sub-county, the study revealed that most business operators got information on the KBA initiative through mass media (Radio, Television, and Newspaper). It can be concluded that other sources of information, e.g., Information, Education, and communication material (IEC), pamphlets distributed by KBA, and formal KBA campaign initiatives are not common among the respondents.

5.4.3 To assess the perception of small business operators on effectiveness of strategies employed by the Kenya Bankers Association initiative "Kaa Chonjo" in curbing cybercrime.

In assessing the effectiveness of strategies employed by the Kenya Bankers Association initiative "Kaa Chonjo" in curbing cybercrime, the study revealed that the KBA initiative was directly effective in raising awareness of cybercrime among small business operators in Kasrani Sub-county. This meant that an increase in the KBA strategies led to increased cybercrime awareness hence being very effective in curbing cybercrime. The more the KBA strategies to increase cybercrime awareness, the more it leads to decreased cybercrime incidents.

5.5 Recommendations

Based on the findings of this study, there are key recommendations surrounding the area of cybercrime, ICT adoption, and the Kenya Bankers Association initiative:

5.5.1 Extent to Which Small Business Operators Have Adopted Use of ICT in Their Businesses

The study recommends that small business operators adopt modern technologies to increase productivity in their operations. Also, business operators are encouraged to adopt cybersecurity measures to help curb cybercrime.

5.5.2 Assessing cybercrime awareness level among the small business operators in Kasarani sub-county, Nairobi

The study recommends that cybercrime awareness be increased within business operations to avoid falling victim to cybercrime incidents. The KBA cybercrime campaigns should target more small business operators since they rely on cyberspace to conduct their businesses with very limited knowledge on cybercrime prevention strategies in place.

5.5.3 To assess the effectiveness of strategies employed by the Kenya Bankers Association initiative "Kaa Chonjo" in curbing cybercrime.

The study recommends that KBA should increase the initiative to increase awareness among small business operators. Also, other sources of information, e.g., Information, Education, and communication material (IEC), pamphlets distributed by KBA, and formal KBA campaign initiatives, are not common among the respondents.

One of the finding indicated that KBA’s cybercrime prevention campaigns contributed to 15.7 percent of the variations in the cybercrime awareness. This study

recommends that KBA needs to apply more strategies that will ensure that majority of the population are aware about the cybercrime prevention. It also need to carry out targeted campaigns to small business people since over 60 percent in Kasarani Sub-county have not been trained on cybercrime prevention. More trainings will lead to more awareness.

5.6 Areas for Further Research

First, the study analyzed respondents through mobile phone usage. Future studies should include operations over other technological devices, e.g., computers.

Secondly, the study respondents were limited to the Kasarani sub-county. This means that the selected respondents were limited to this area and left others. Future studies should put this into consideration and go further to analyze respondents from the larger geographical area.

Thirdly, the current study used quantitative method in data collection. Future studies should use qualitative approach which would offer more details on the effectiveness of the Kenya Bankers Association's cybercrime awareness campaigns.

REFERENCES

Aiken, M., Mc Mahon, C., Haughton, C., O'Neill, L., & O'Carroll, E. (2016). A consideration of the social impact of cybercrime: examples from hacking, piracy, and child abuse material online. *Contemporary Social Science*, *11*(4), 373-391.

Al-Rahmi, W. M., Yahaya, N., Aldraiweesh, A. A., Alamri, M. M., Aljarboa, N. A., Alturki, U., & Aljeraiwi, A. A. (2019). Integrating technology acceptance model with innovation diffusion theory: An empirical investigation on students' intention to use E-learning systems. *Ieee Access*, *7*, 26797-26809.

Amin, J., Thompson, B., Ariu, D., Giacinto, G., & Fabio Roli, P. K. (2015). *"2020 Cybercrime Economic Costs: No Measure No Solution" 2015 10th International Conference on Availability, Reliability and Security 2015*. Retrieved from giacintodie.unica.it

Bada, M., Solms, B. V., & Agrafiotis, I. (2012). *Reviewing National Cybersecurity Awareness in Africa: An Empirical Study*. Retrieved from Core: https://core.ac.uk/reader/211243124

Bajaj, A. K., & Jyoti, C. (11/03/2015, 03 11). *Cyber Crime through Mobile Phone in India and Preventive Methods*. Retrieved from International Journal of Research and Review:https://www.researchgate.net/publication/327436826_Cyber_Crime_through_Mobile_Phone_in_India_and_Preventive_Methods

Berry, C. T., & Berry, R. L. (2018). An initial assessment of small business risk management approaches for cyber security threats. *International Journal of Business Continuity and Risk Management*, *8*(1), 1-10.

Brookins, M. (2019, March 07). *Impact of Technology on Small Business*. Retrieved from Chron Newsletter: https://smallbusiness.chron.com/impacts-technology-small-business-2190.htm

Brown, J. D. (2009). *Applied Communication: Communication and Health Systems*. New York and London: Routledge.

Charness, N., & Boot, W. R. (2016). Handbook of the Psychology of Aging (Eighth Edition). *ScienceDirect*, 389-407.

Chen, H., Rong, W., Ma, X., Qu, Y., & Xiong, Z. (2017). An Extended Technology Acceptance Model for Mobile Social Gaming Service Popularity Analysis. *Internet of Everything*, 1-12.

Chen, H., Rong, W., Ma, X., Qu, Y., & Xiong, Z. (2017). An Extended Technology Acceptance Model for Mobile Social Gaming Service Popularity Analysis. *Internet of Everything*, 1-12.

Chen, J. (2016). Cyber Security: Bull's-Eye on Small Businesses. *J. Int'l Bus. & L.*, *16*, 97.

Chin, A. G., Harris, M. A., & Brookshire, R. (2018). A bidirectional perspective of trust and risk in determining factors that influence mobile app installation. *International Journal of Information Management*, *39*(May 2017), 49–59. https://doi.org/10.1016/j.ijinfomgt.2017.11.010

Chung, I. J. (2018). Dynamics of media hype: Interactivity of the media and the public. In P. Vasterman, *From Media Hype to Twitter Storm* (pp. 211-228). Amsterdam: Amsterdam University Press.

Chung, I. J. (2018). *Dynamics of media hype: Interactivity of the media and the public. In P. Vasterman*, From Media Hype to Twitter Storm (pp. 211-228). Amsterdam: Amsterdam University Press.

Communication Authority. (2021, January 2). *Communication Authority of Kenya.* Retrieved from https://www.ca.go.ke/cyber-threats-on-the-rise-with-increased-reliance-on-icts-in-the-mitigation-of-covid-19-pandemic.

Dwivedi, P. K., & Pandey, I. (2013). Role of Media in Social Awareness. *International Journal of Humanity and Social Sciences Vol (01)*, 67-70.

Finaccess. (2019). *Findings for Finaccess 2019*, 1-12

Gaziano, C. (2019). Knowledge Gap Hypothesis and Journalism. *The International Encyclopedia of Journalism Studies*, 1-7.

Gaziano, C., & Gaziano, E. (2014). Theories and methods in knowledge gap research. In *An integrated approach to communication theory and research* (pp. 136-150). Routledge.

Harris, M. A., Brookshire, R., & Chin, A. G. (2016). Identifying factors influencing consumers' intent to install mobile applications. *International Journal of Information Management, 36*(3), 441-450.

Internet World Stats. (2019, June 30). Internet World's Stats Usage and Population Statistics. Retrieved from Internet World Stats: https://www.internetworldstats.com/stats1.htm

Internet World Stats. (2019, June 30). *Internet Worls Stats Usage and Population Statistics*. Retrieved from Internet World Stats: https://www.internetworldstats.com/stats1.htm

ITU. (2019). *Global and Regional ICT data*. Retrieved from ITU website: https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

Jones, B. H., Chin, A. G., & Aiken, P. (2014). Risky Business: Students and Smartphones. *Tech Trends*, 73-83.

Jones, B. H., Chin, A. G., & Aiken, P. (2014). Risky Business: Students and Smartphones. *Tech Trends*, 73-83.

Kang, R., Dabbish, L., Fruchter, N., & Kiesler, S. (2015). "My Data Just Goes Everywhere:" User Mental Models of the Internet and Implications for Privacy and Security. In *Eleventh Symposium On Usable Privacy and Security ({SOUPS} 2015)* (pp. 39-52).

Karibu, J. (2018). *Cybercrime Statistics in Kenya (2018)*. Retrieved from www.kenyakwanza.com/cyber-crime-statistics.in-kenya-2018

Karibu, J. (2018). Cybercrime Statistics in Kenya (2018). Retrieved from www.kenyakwanza.com/cyber-crime-statistics.in-kenya-2018

Kemb, S. (2022, February 15). *Datareportal*. Retrieved from Digital 2022: Kenya: https://datareportal.com/reports/digital-2022-kenya.

Kenya National Bereau of Statistics. (2019). *2019 Population and Housing Census Results.* Nairobi: KNBS.

Khan, Z. C., & Mkuzangwe, N. N. (2022). Advancing cybersecurity capabilities for South African organisations. *Proceedings of the 17th Conference on Information Warfare*

and Security, 2022 (pp. 102-110). Pretoria, South Africa: International Council For Scientic and Industrial Research.

Kohar, A., Riadi, I., & Lutfi, A. (2015). Analysis of Smartphone Users Awareness Activities Cybercrime. *International Journal of Computer Applications*, *129*(2), 1-6.

Kombo and Tromp (2006), *Research Tools 3rd edition*, Jaico Publishing House, New Delhi, India.

Kothari, C. R. (2004). *Research Methodology Methods and Techniques (Second Revised Edition).* New Delhi: New Age International Publishers.

Koyuncu, M., & Pusatli, T. (2019). Security Awareness Level of Smartphone Users: An Exploratory Case Study. *Mobile Information Systems*, *2019*.

Kritzinger, E., Bada, M., & Nurse, J. R. (2017). *Kent Academic Repository*. Retrieved from A study into the cybersecurity awarenessinitiatives for school learners inSouth Africa and the U: https://core.ac.uk/reader/189720737.

Ksherti, N. (2019). Cybercrime and Cybersecurity in Africa. *Journal of Global Information Technology and Management*, 77-81.

Kshetri, N. (2015). Cybercrime and cybersecurity issues in the BRICS economies. *Journal of Global Information Technology Management*, 18(4), 245-249.

Kumar, P., Naik, S. M., Devkar, U. R., Chetty, M., Clegg, T. L., & Vitak, J. (2017). 'No Telling Passcodes out Because They're Private': Understanding Children's Mental Models of Privacy and Security Online. *Proceedings of the ACM on Human-Computer Interaction*, *1*(CSCW), 64.

Lamorte, W. W. (2019, September). *Diffusion of Innovation Theory*. Retrieved from Behavioral Change Model: phweb.bumc.bu.edu/otlt/MPH-Modules/SB/BehavioralChangeTheories/BehavioralChangeTheories4.html

Markelj, B., & Bernik, I. (2015). Safe use of mobile devices arises from knowing the threats. *Journal of information security and applications*, *20*, 84-89.

Masood, T., & Sonntag, P. (2020). Industry 4.0: Adoption challenges and benefits for SMEs. *Computers in Industry*, *121*, 103261. https://doi.org/https://doi.org/10.1016/j.compind.2020.103261

Mbogo, A. (2018). *KBA Launches the Annual Kaa Chonjo Awareness Campaign to Boost Security of Payment Platforms*. The Kenyan Wall Street. https://kenyanwallstreet.com/kba-launches-the-annual-kaa-chonjo-awareness-campaign-to-boost-security-of-payments-platforms/

McCombs, M. E., Shaw, D. L., & Weaver, D. H. (2013). *Communication and democracy: Exploring the intellectual frontiers in agenda-setting theory*. Routledge.

Meier, Y., Schäwel, J., & Krämer, N. C. (2020). The shorter, the better? Effects of privacy policy length on online privacy decision-making. *Media and Communication, 8*(2), 291–301. https://doi.org/10.17645/mac.v8i2.2846

Mikami, S., Takeshika, T., & Kawabata, M. (2011). Influence of the Mass media on the Public awareness of global environmental issues in Japan. *Asian Geographer: Volume 18, 1999 - Issue 1-2: Eco-consciousness in Asia and the Pacific* , 87-97.

Morgan, S. (2019). *2019 Official Annual Cybercrime ReportSteve Morgan, Editor-in-ChiefCybersecurity VenturesCybercriminal activity is one of the biggest challenges that humanity will face in the next two decades*. Retrieved from Herjavec Group: https://www.herjavecgroup.com/wp-content/uploads/2018/12/CV-HG-2019-Official-Annual-Cybercrime-Report.pdf

Mugenda, A. A. (2003). *Research Methods in Quantitative and Qualitative Approaches,* Nairobi: Acts Press, Kenya

Muhati, E. (2018). Factors affecting cyber-security in Kenya – A Case of Small Medium Enterprises (Thesis). Strathmore University. Retrieved from http://suplus.strathmore.edu/handle/11071/6013.

Mutia, C. K. (2020). *Access to Credit and Household Savings in Kenya Evidence From Kenya National Finaccess 2019 Survey* (Doctoral dissertation, University of Nairobi).

National Crime Research Centre. (2019). *Transport and Security Challenges in Kenya.* Nairobi: NCRC.

Nazari, F., Khosravi, F., & Babaihavaeji, F. (2013). Applying Rogers' Diffusion of Innovation to the acceptance of online database at Universirty Zone of Iran. *Malaysian Journal of Library & Information Science Vol 18 no. 3*, 25-28.

Nelly Awinja, N., & Isola Fatoki, O. (2021). Effect of Digital Financial Services on the Growth of SMEs in Kenya. *African Journal of Empirical Research*, *2*(1), 79–94. https://doi.org/10.51867/ajer.v2i1.16

Newton, K. (2010). Mass Media Effects: Mobilization or Media Malaise? *British Journal of Political Science: Coverage*: 1971-2013 (Vol. 1, No. 1 - Vol. 43, No. 4), 577-599.

Nzeakor, O. F., Nwokeona, B. N., & Ezeh, P.-J. (2020). Pattern of Cybercrime Awareness in IMO State Nigeria: An Empirical Assessment Vol14 Issue January-June 2022. *International Journal of Cyber Criminology*, 223-229.

OECD (2004), "ICT, E-Business and Small and Medium Enterprises", *OECD Digital Economy Papers*, No. 86, OECD Publishing, Paris, https://doi.org/10.1787/232556551425.

Okuku, A., Renaud, K., & Valeriano, B. (2015). Cybersecurity Strategy's Role of raising Kenyan awareness of mobile security. *Information & Security: An International Journal*, 3207-20.

Omar, M., & Dawson, M. (2013, April). Research in progress-defending android smartphones from malware attacks. In *2013 third international conference on advanced computing and communication technologies (ACCT)* (pp. 288-292). IEEE.

Osiejewicz, J. (2017). Education on cyber security issues under European Union law. A standard of personal data protection. *Development of Jurisprudence Problems and Prospects*, 73-76.

Parker, F., Ophoff, J., Van Belle, J. P., & Karia, R. (2015, November). Security awareness and adoption of security controls by smartphone users. In *2015 Second international conference on information security and cyber forensics (InfoSec)* (pp. 99-104). IEEE.

Potter, J. (2012). *Media Effects.* California: Sage Publishers.

Rotich, E. K. (2020). *Cyber Terrorism and National Security in Africa: a Case Study of Kenya* (Doctoral dissertation, university of Nairobi).

Rotich, K. (2021, February 10). Cybercrime Attacks on Kenya Organizations. *Business Daily*, p. 1.

Safavi, S., Shukur, Z., & Razali, R. (2013). Reviews on cybercrime affecting portable devices. *Procedia Technology*, *11*, 650-657.

Sampei, Y., & Aoyagi, M. (2001). Mass-media coverage, its influence on public awareness of climate-change issues, and implications for Japan's national campaign to reduce greenhouse gas emissions. *Global Environmental Change Vol 17, Issue 2*, 16-2.

Sampei, Y., & Aoyagi-Usui, M. (2009). Mass-media coverage, its influence on public awareness of climate-change issues, and implications for Japan's national campaign to reduce greenhouse gas emissions. *Global Environmental Change*, *19*(2), 203-212.

Shah, M. H., Jones, P., & Choudrie, J. (2019). Cybercrimes prevention: promising organisational practices. *Information and Knowledge Management: Volume: 32 Issue: 5*, 1125-1129. Retrieved from Vol. 32 No. 5, pp. 1125-1129. https://doi.org/10.1108/ITP-10-2019-564.

Statista (2019, May). *Demographics and Use*. Retrieved from Statista: https://www.statista.com/statistics/505883/number-of-internet-users-in-african-countries/

Statista. (2022, May). *Share of web traffic in Kenya as of May 2022, by device*. Retrieved from Statista Website: https://www.statista.com/statistics/1312186/web-traffic-by-device-in-kenya/

Sterwart, F. (nd). *Development and Security.* Centre for Research on Inequality, Human Security and Ethnicity, CRISE : Queen Elizabeth House, University of Oxford.

Weijer, S. G., Leekfeldt, R., & Zee, S. V. (2021). Cybercrime Reporting Behavior Among Small-and Medium-Sized Enterprises in the Netherlands. In M. W. Kranenbarg, & R. Leukfeldt, *Cybercrime Reporting Behaviors Among Small-and-Medium-Sized Enterprises in th Netherlands* (pp. 303-324). Hague: Springer.

Wolfe, M., Jones, B. D., & Baumgartner, F. R. (2013). A failure to communicate: Agenda setting in media and policy studies. *Political Communication*, *30*(2), 175-192.

Wright, J., Dawson Jr, M. E., & Omar, M. (2012). Cyber security and mobile threats: The need for antivirus applications for smart phones. *Journal of Information Systems Technology and Planning*, *5*(14), 40-60.

Zulkefli, Z., Singh, M. M., Shariff, A. R. M., & Samsudin, A. (2017). Typosquat Cyber Crime Attack Detection via Smartphone. *Procedia Computer Science*, *124*, 664-671.

APPENDICES

APPENDIX I: QUESTIONNARE

Questionnaire No: …….. Date: …….

Dear Respondent,

My name is Peter Omusula, a student at United States International University-Africa, conducting a research for my Master of Arts in Communication Studies degree. This research is a requirement for me to graduate. I, therefore, request you to spare about 10 minutes of your time to respond to the following questions to the best of your knowledge. The information you provide will be treated confidentially and used for academic purposes only. To guarantee confidentiality, you are not required to state your name anywhere in this questionnaire.

SECTION A: QUESTION

1. What business are you involved in? …….

2. Do you use your mobile phone device in your business?

   i. Yes [ ]

   ii. No [ ]

3. For what purpose do you use your mobile phone?

Purpose	**Yes**	**NO**
Checking and replying Emails		
Socializing		
Research		
Shopping		
Search of information		
Search of information		
Downloading Music &Movies		
Gambling		
Banking		
Auction		
Any others (Please specify)_____		

4. What factors have influenced the use of mobile phone technology in your operations/business?

   ……

B. Cybercrime awareness level

5. Among the following cybercrime incidences which one have you experienced within the last one year? (The incidences can be more than one)

Purpose	**Yes**	**NO**
Denial of Service		
Hacking		
Identity theft		
Data Theft		
Any others (Please specify)_____		

6. To what extent do you agree with the following statements on the level of awareness about cybercrime issues?

Key; **5 -Strongly Agree, 4 -Agree, 3 -Undecided, 2 - Disagree, 1 -Strongly Disagree**

Statements	**Strongly Disagree**	**Disagree**	**Undecided**	**Agree**	**Strongly Agree**
I only install mobile application that are trusted over my phone					
Before installing application I usually read application provider's privacy and policy for using applications					
I usually store most of my credential/documents over my phone					
I usually use free wi-fi whenever I access one for my businesses to save on my data					

Others (specify)

_____

_____

C. Cybercrime prevention strategies

7. To what extent do you agree with the following statements on Kenya Bankers Association campaign ("Be alert," / "Kaa Chonjo" strategy on cybercrime awareness?

Key; **5 -Strongly Agree, 4 -Agree, 3 -Undecided, 2 - Disagree, 1 -Strongly Disagree**

Statements	**Strongly Disagree**	**Disagree**	**Undecided**	**Agree**	**Strongly Agree**
I heard cybercrime prevention strategy dubbed "Kaa Chonjo" through the mass media (Radio, Television and Newspaper)					
I got the information on cybercrime prevention through Information, Education, and communication material (IEC) distributed to me by the Kenya Bankers association/associates					
I learnt about cybercrime prevention through pamphlets distributed by the Kenya Association of Bankers					
I learnt about cybercrime prevention through the formal campaign initiative by Kenya Bankers Association that I have participated in					

Others (specify)

_____

_____

_____

8. To what extent do you agree with the following statements on impact of the media on cybercrime

Key; **5 -Strongly Agree, 4 -Agree, 3 -Undecided, 2 - Disagree, 1 -Strongly Disagree**

Statements	**Strongly Disagree**	**Disagree**	**Undecided**	**Agree**	**Strongly Agree**
Media has informed me of the tricks that are used by criminals involved in cybercrime					
Media has informed me on the measures to take to avoid cases of cybercrime within my business					
Media has made me to know steps to take prevent a cyberattack on my internet device					
Since being informed by the media on cybercrime, I have not been a victim					

Others (specify)

_____

SECTION II: SPECIFIC INFORMATION

9. Gender

   Male [ ]

   Female [ ]

10. Age

    18-30 years [ ]

    30-40 years [ ]

    Over 40 years [ ]

11. What is your highest Level of education?

    Primary [ ]

    Secondary [ ]

    College [ ]

    University [ ]

    None [ ]

12. For how long have you operated your business in Kasarani constituency?

    Less than 6 months [ ]

    6-12 months [ ]

    Over 1 year [ ]

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

    Yes [ ]

    No [ ]

APPENDIX II: IRB LETTER

United States International University-Africa

USIU-A/IRB/223-2020 **USIU-A Institutional Review Board (IRB)**

12th June 2020

Peter Omasula
United States International University-Africa
pomasula@usiu.ac.ke

Dear Peter,

IRB-RESEARCH APPROVAL

The USIU-A IRB has reviewed and granted an ethical approval for the research proposal titled **"Effectiveness of Online Safety Awareness Campaign Strategies by Kenya Bankers Association; Kasarani Sub-County, Nairobi".**

The approval is for **twelve months** from the date of IRB. A continuing review application must be approved within this interval to avoid expiration of IRB approval and cessation of all research activities. A mid-term report and a final report must be provided to the IRB within the twelve months approval period. All records relating to the research (including signed consent forms) must be retained and available for audit for at least 3 years after the research has ended.

You are advised to follow the approved methodology and report to the IRB any serious, unexpected and related adverse events and potential unanticipated problems involving risks to subjects or others.

Should you or study participants have any queries regarding IRB's consideration of this project, please contact irb@usiu.ac.ke

Sincerely,

RESEARCH OFFICE

Dr. Juliana Nzamula
IRB chair
Tel: +254 730 116 628
Email: jnzamula@usiu.ac.ke

APPENDIX III: NACOSTI LETTER

United States International University-Africa

National Commission for Science Technology and Innovation
P. O. Box 30623, 00100,
Nairobi, KENYA.

12th June 2020

Dear Sir/Madam

REF: PERMISSION TO CONDUCT RESEARCH: PETER OMUSULULA
STUDENT ID NO. 649148

The bearer of this letter is a student of United States International University (USIU) -Africa pursuing **Master of Arts in Communication Studies.**

As part of the program, the student is required to undertake a dissertation on **"Effectiveness of Online Safety Awareness Campaign Strategies by Kenya Bankers Association; Kasarani Sub-County, Nairobi."** which requires the Student to Collect Data. His proposal has been subjected to ethical review and positive verdict given by the Institutional Review Board.

Kindly assist the student with the research permit and should you have any queries contact the undersigned.

Yours Sincerely,

Prof. Amos Njuguna,
Dean, School of Graduate Studies, Research and Extension
Tel: 730 116 442
Email: [illegible]

p.o box 14634-00800 Nairobi, Kenya | tel:254-730-116-000 | info@usiu.ac.ke
www.usiu.ac.ke