UNIVERSITY OF CAPE COAST

EXAMINING THE PERCEIVED VULNERABILITY AND EXPERIENCES OF INBOUND TOURISTS ON CYBERCRIME IN GHANA.

BY

MILLICENT DADSON

Thesis submitted to the Department of Hospitality and Tourism Management of the Faculty of Social Science, College of Humanities and Legal Studies, University of Cape Coast in partial fulfillment of the requirements for the award of a Master of Philosophy degree in Tourism Management.

JULY 2019

DECLARATION

Candidate's Declaration

I hereby declare that this thesis is the result of my own original work and that no part of it has been presented for another degree in this University or elsewhere.

Name: Millicent Dadson

Candidate's Signature: …………………..…. Date: ………………………...

Supervisor's Declaration

I hereby declare that the preparation and presentation of the thesis were supervised in accordance with the guidelines on the supervision of thesis laid down by the University of Cape Coast

Name: Prof. Kwaku A. Adutwum Boakye

Supervisor's Signature: ……………………. Date: …………………….

ABSTRACT

Although Information and Communication Technology (ICT) applications have become essential to the operations in the tourism industry but its benefits accruing to the growing importance is also being challenged by cyber criminals and online intruders. There has been surprisingly little effort to understand the perceived vulnerability and experiences in the context of tourism. Therefore, this study explored the perceived vulnerability and experiences of inbound tourists' on cybercrime in Ghana. The study used a cross-sectional design with quantitative approach for data collection and analysis. A convenience sampling technique was employed to select 400 inbound tourists who visited Ghana from 1st November to 1st January which was the period for data collection. The study was guided by the Routines Activity Theory. The findings of the study proved that both cybercrime victimization and perceived vulnerability of inbound tourists in Ghana is quite low. Again, it was revealed that inbound tourists that visit Ghana do consider the issue of cybercrime when planning for their trips meanwhile their rejection of a particular destination for alternative destinations has never been on the issue of cybercrime. Respondents were also well aware of cybercrime preventive strategies. Evidently however, level of education was found to have relationship with respondents' perceived vulnerability while trip experiences and purpose of visitation also associated with respondents' cybercrime victimization.

ACKNOWLEDGEMENTS

I thank the Lord almighty for making all things possible and with whom this thesis has seen the light of the day. I appreciatively acknowledge my supervisor: Professor Kwaku A. Adutwum Boakye whose commitment, guidance, contributions, support, constructive criticisms, and suggestions have fine-tuned the outcome of this research. My next appreciation goes to Dr. Mrs. Fay Amissah Eunice for her immeasurable support, words of encouragement and assistance when things were tough in my course of study. I further wish to extend my deepest gratitude to Dr. Adongo for all the guidance, assistance and your insightful comments offered me. I would also like to thank all the lecturers of the Department of Hospitality and Tourism Management for their inputs during my presentations.

I want to render my profound gratitude also to Samuel of Kakum National Park, Martin, Aziz and Michy of Hans Cottage Botel and the rest for helping me out despite their busy schedules. Finally, my sincere appreciation to my family and friends especially Timothy Terry Tweneboah, Abraham Appiah, Lydia Kumi Gyimah, and to all those who assisted in diverse ways towards the completion of this work, but whose names I could not mention, God richly bless you all.

DEDICATION

To my late grandmother, Madam Sarah Ekua Afoamah Gyamenah.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

Figure **Page**

LIST OF ACRONYMS

ATM	:	Automated Teller Machine
CSIS	:	Center for Strategic and International Studies
CSI	:	Computer Security Institute
CID	:	Criminal Investigation Department
CRS	:	Central Reservation System
CCTV	:	Closed Circuit Television
CERT	:	Computer Emergency Response Team
CC	:	Cybercrime
CCV	:	Cybercrime Victimization
GDS	:	Global Distribution System
GTA	:	Ghana Tourism Authority
ICT	:	Information Communication Technology
ISC	:	Information Security Congress
IDS	:	Intrusion Detection System
ITU	:	International Telecommunication Union
IRB	:	Institutional Review Board
LET	:	Lifestyle Exposure Theory
RFID	:	Radio Frequency Identification
SMS	:	Short Message Service
SIM	:	Subscriber Identification Module
UNWTO	:	United Nations World Tourism Organizations
VPN	:	Virtual Private Network

CHAPTER ONE

INTRODUCTION

Background to the Study

Different types of crime are committed against tourists including; theft, assault, robbery, rape, piracy, larceny, and even kidnapping and murder (Pizam & Mansfield, 2006). In the view of Adam and Adongo (2016), the attention received by tourists' related crimes particularly in the digital media has called for the need of every Destination Management Organizations (DMO's) to be concerned with tourists-related crimes. Even though studies into crime on tourists is not new (Boakye, 2010; Brunt, Mawby & Hambly, 2000), but since crime against tourists comes in different forms and context, there is the need to be concerned with these varying forms of crime tourists suffer such as cybercrime. According to Magliulo (2016), the competitiveness of every tourism destinations depends on several factors, including security. This is why Holcomb and Pizam (2006) captured in their study that, destinations which are perceived to be crime ridden and (for that matter) insecure, lose out to attract tourist dollars.

All over the world, people, companies, nations and societies are becoming increasingly dependent on Information and Communication Technologies (ICT) in respect to the improvements in the quality of life of people and the communities in which they live (Osei-Bryson & Ngwenyama, 2014). And so, the tourism industry, like many others is also embracing the use of Information Communication Technology (ICT) (Olding & Turner, 2007). The industry is known as an information intensive one (Cox, Burgess, Sellitto & Buultjens, 2009) that relies on the communication with tourists through various channels either to market their products or to build customer relationships (Poon, 1993).

ICTs are now mediating the experiences of tourists making them more innovative than before (Kim 2013). In the views of Gretzel and Jamal (2009), ICT's have become essential features of the creative lifestyle and experiences of the contemporary tourist most especially with the use of mobile devices and other transportable smart computers. Studies (Tussyadiah & Zach 2012; Wang, Park, & Fesenmaier 2012) have documented the impact of the use of ICT (especially smartphones) on different aspects of the tourist experiences including information search, travelers' use of smartphones on idle times such as waiting for bus, on-site decision making, documentary and sharing of experiences. The tourists live their lives on ICT just as the ordinary individual through the use of smartphones, laptops and hard-drives, credit cards, the internet and the destinations' Wi-Fi which helps to enhance their satisfaction during their holiday making (Osei-Bryson & Ngwenyama, 2014).

The use of technology has also got disadvantages including data breach and information loss (Cobanoglu & Demicco, 2007). Other problems such as computer-assisted fraud, espionage, sabotage, vandalism, hacking, system failures, have been possible because of the existence of the cyber space (Cobanoglu & Demicco, 2007). Aside the importance of technological devices, people who want to cut corners to gain power and money have tend towards using information technologies and its devices to commit crimes, herein, the term "cybercrime" becomes evident (Cobanoglu & Demicco, 2007). According to Britz (2009), cybercrime has emerged as a salient area of inquiry for criminologists and a growing concern for public policy over the years.

In 2010, Ghana had its reputation tarnished by being ranked among the top 10 countries in the world where cybercrime is most prevalent (Ghana Business News Dec 2nd, 2010). Kwablah (2009) indicated that, the issue of Ghana’s status on cybercrime has impacted negatively on the country’s image in the global environment. Kwablah also revealed that many companies in the western world have blacklisted credit card transactions coming from Ghana. Secondly, Ghana was the second most frequently blocked location by U.S e-commerce sites because retailers are skeptical about fake orders from internet scammers.

Again, Bokpe (2013) also indicated that, due to concerns for international e-commerce and fraud, as high as 76 percent and 58 percent of U.S. and Canadian merchants who accepted international orders online shut off orders from Nigeria and Ghana respectively in 2008. Baker and Stockton (2014) asserted that, crimes committed against the travel and tourism industry affect tourism by damaging the destination’s image and instilling fear in potential tourists.

Tourists become vulnerable to cybercrime as the destination through the use of Wi-Fi in the various facilities they patronize; aviation, resort, hotels, attraction sites, malls, among others (Nayak, 2016). According to Nayak (2016), the hospitality and tourism industry is dependent upon wireless communications and as a result, faces a higher risk of security vulnerabilities. The use of the internet and wireless networks such as Bluetooth and Wi-Fi has the potential to open doors to cyber criminals and allows unauthorized entry of privacy hackers thereby putting tourists’ privacy at a risk at the destination.

Cybercrime ranks third behind government corruption and narcotics as far as global economic impact of cybercrime is concerned (McAfee, 2017), since it touches everyone and has a low risk to high payoffs. The impact of cybercrime amounts to more than the income of almost all but a few countries. Considering the cost of cybercrime in relation to the worldwide internet economy, it estimated $4.2 trillion in 2016. This fact can make cybercrime be viewed as a 14% tax on economic growth (McAfee, 2017).

Nakashima and Peterson (2014) in their national security report estimated that, the likely annual cost of cybercrime to the world's economy is more than $445 billion or almost 1 percent of global income. Cybercrime is ranked with the likes of offences such as drug trafficking in terms of worldwide economic harm, Center for Strategic and International Studies (CSIS) (2017). CSIS in their 2017 report revealed that, United States lost about $100 billion, Germany was second with $60 billion, and China followed with $45 billion in areas like cyber espionage, credit card fraud, identity theft, intellectual property theft, among others.

According to Lan, Murugi, Ding and Qin (2018), the cost of Cyber-crime in Africa in 2017 was estimated at $3.5 billion, a rise from 2016, where African countries were estimated to lose at least $2 billion in cyber-attacks. The report described 2017 as a tough period for local organizations. The number of threats and data breaches increased with a clear evidence that home grown cyber criminals were becoming more skilled and targeted. Nigeria led the pack in Africa with an estimated cost of cybercrime in 2017 being $649 million with the number of certified professionals standing at 1800. The other top four victims of the daring cyber-attacks over $3billion loss for the whole Africa during the year were Ghana, Kenya, Tanzania and Uganda (Lan et al., 2018).

A report by Kenyan-based IT firm, Serianu Limited, revealed that the Ghanaian economy lost a total of US$50 million to cybercrime in 2016 compared to US$69million in 2017 and US$97million 1n 2018, (director of Cybercrime Unit, Ghana Police Service; Dr. Gutstav Yankson on Ghanaweb Business News, 11th Oct 2018). Also, the communication minister (Ursula Owusu) on Ghanaweb general news on 26th Oct 2018 also emphasized that, the fight for internet security is a responsibility for all; consumers, travellers, government and the cyber workforce.

Cyber-criminals are causing their victims emotional, physical and financial trauma, an expert claimed at the Information Security Congress (ISC) in Orlando, Florida, on (September, 2016). During the congress, Howard, a participant of the congress told her audience "You would be surprised at the levels of trauma suffered by cybercrime victims," In nine out of ten cases, there is a financial loss to the victim, a loss which gets even greater when stolen data is sold, "Victims often feel that there has been an invasion of their privacy "People feel victimized, that they've suffered a traumatic experience". It is the very same feelings that victims of assault experience. They're upset, depressed, they feel guilt", victims can suffer insomnia and sometimes eating disorders.

Travellers' perceptions on a particular destination are formed in relation to their expectations, previous experiences, information from friends and relatives, the internet, the news/media, marketing information and information from travel agencies (Kotler, Bowen & Markens, 2006). According to Tarlow (2006 & 2009), Breda and Costa (2006) and a host of other authors, tourism is one sector which is largely influenced by perceptions (especially of security) which, ultimately, determine the attractiveness or otherwise of destinations. Hence, security (or at least perceptions of it) constitutes one key prerequisite for the appeal of a destination. The safer (and more crime-free) a destination is perceived to be, the more likely it is to be chosen as a potential holiday destination and vice-versa. Also, the consideration of this gap in the research literature is imperative since the Internet and other information and communication technologies (ICTs) are becoming increasingly significant in the tourism industry (Buhalis & Deimezi, 2003).

Statement of the Problem

According to Boakye (2012), studies on tourists' security are of vital importance for countries that benefit immensely from tourism patronage like Ghana. This is because; there exist a potential loss of revenue in a situation of a country being 'blacklisted' as an unsafe destination. Cybercrime has been a major security threat and challenge for Ghana as a tourist destination, and it is important to come out with appropriate measures to combat it Mr Kan Dapaah, Minister of National Security, general news on myjoyonline, (4/4/2017).

Also, certain activities of cybercriminals popularly known as 'sakawa', have been reported (Ministry of Communications, 2014). Thus, some residents and foreigners have become victims of cybercrime activities and threats while in the country. As a result, there have been instances where US Federal Bureau of Investigation (FBI), (2015) and the United Kingdom Foreign Commonwealth Office Travel Advisory (2015) alerted their citizens travelling to Ghana and other affected countries in sub-Saharan Africa to be cautious of using mobile phones and free Wi-Fi connections.

Despite the relevance of investigating the issue of cybercrime within the tourism context in Ghana, there are significant research gaps in this area that needs to be addressed. Firstly, the findings by Kwablah, (2009) on online scammers in Ghana revealed that, these scammers see Westerners as their prime target and justify their duping of Westerners by claiming that it is pointed retribution for centuries of historical injustices perpetrated by the West against Africans. Meanwhile, these same westerners happen to be the tourists and potential market for Ghana as a tourists' destination. Based on these media reports and empirical findings, it could be seen that Ghana has already been regarded as a cybercrime prevalent country which has gained global attention especially after it was ranked 7th in the world and 3rd in Africa where cyber-attacks originate. Meanwhile, empirical research into this issue is limited. Thus, tourism researchers are yet to explore the perceived vulnerability of inbound tourists and their experiences on cybercrime.

In relation to literature, even though some studies (Boakye, 2012; George 2010) have looked at crime perpetrated against tourists with the emphasis on traditional crimes but studies on cybercrime perpetrated against tourists are limited. Significantly however, past studies (e.g. Kim, Qu, & Kim, 2009; Park & Tussyadiah, 2016) have also been principally interested in investigating perceived risk towards information technology (such as security and privacy) in travel and tourism. As well, the physical risk in the usage of the smartphones at the destination including the theft of mobile devices have also been investigated (Khan, Abass, & Al-Muhtadi, 2015). The integration of destination related risks thus, destination-infrastructure and physical risks have also been studied (Dayour, Kimbu & Park 2017) with critical consideration on only backpackers. Thus, it can be argued that the perceived vulnerability and experiences of inbound tourists on the cyber space in the destination is equally important to be investigated.

As a matter of fact, a number of cybercrime studies have concentrated on cybercrime but either in different context such as the banking, education, e-commerce and communication sectors (Abem 2013; Boateng, Longe, Mbarika & Isabalija 2010) or in the perspective of law enforcement agencies and the perpetrators (Kwablah, 2009 & Warner, 2011). Little is known about cybercrime within the context of tourism; meanwhile, looking at it from this perspective is also necessary because, the study by Mansfeld and Pizam (2006) has confirmed that tourists increasingly consider issues of physical safety for example cybercrime when making choices between tourist destinations.

Noticeably however, there has been very little empirical investigation discussion on the potential threats posed by cyber vulnerabilities. The limited information on the views of tourists on cybercrime in Ghana has been a motivating factor for carrying out this research.

Research Questions

This study therefore seeks to answer the following questions:

- Are inbound tourists vulnerable to cybercrime in Ghana?
- Does the perceived vulnerability of inbound tourists to cybercrime shape their travel decisions?
- What are some of the cybercrime incidents experienced by tourists in Ghana?
- What are the preventive mechanisms adopted by inbound tourists?

- Does any relationship exist between perceived vulnerability and background characteristics of inbound tourists?

Research Objectives

The main objective of the study is to examine the perceived vulnerability and experiences of inbound tourists on cybercrime in Ghana.

Specifically, the study seeks to;

- Examine the perceived vulnerability of inbound tourists on cybercrime in Ghana.
- Analyze how tourists' perceived vulnerability to cybercrime shapes their travel decisions.
- Analyze international tourists' experiences of cybercrime in Ghana.
- Explore international tourists' preventive strategies on cybercrime.
- Explore the relationship between perceived vulnerability and background characteristics of inbound tourists.

Significance of the Study

The findings of this study will contribute to existing literature by bringing to light, tourists' perceived vulnerabilities, actual cybercrime experiences suffered, how perceived vulnerability shapes travel decisions as well as tourists' suggestive preventive strategies which are hitherto not known. This information will be an addition to the body of knowledge on cybercrime on which further studies could be carried out by other researchers to broaden the scope or help serve as baseline for further studies on cybercrime and a foundation for monitoring changes in cybercrime issues in the future.

Also, it is vital that safety and security be tightened to ensure growth and sustainability of the tourism industry within the country since crimes committed against tourists are not a new phenomenon but come with the development of the tourism industry, (Giddens, 1990). Therefore, this study hopes to provide useful information to various stakeholders (such as destination planners and managers) and other interested parties to improve their understanding of what cybercrime is and the various trends of cybercrime situations in Ghana.

For a clearer understanding of cybercrime issues in Ghana, all the parties or bodies concerned (perpetrators, law enforcement agencies and victims') views are all equally important. It is therefore the researcher‘s ultimate aim that the outcome of this study will serve as a guide to policy-makers; government, Ministry of Tourism, Ghana Tourism Authority, and other tourism stakeholders in the policy formulation, in their deliberations on cybercrime and mapping out strategies to address the problem. That is, all cyber vulnerability issues and preventive strategies, as well as actual incidents suffered by tourists will be sorted. With this information, policy makers and the authorities will have a baseline in implementing policies and adopting strategies that will help the tourists on how to protect themselves and limit or avoid any situation of being victimized. For instance, the type of cybercrime tourists experience will help management and tourism planners to design strategies to reduce the incidence of cybercrime. An understanding of the types of cybercrime suffered and suggestive preventive strategies by tourists will better position DMO's to give useful security information to potential inbound tourists as part of their destination marketing activities. Such intervention may enhance the stay of inbound tourists and also improve on the image and reputation of the destination.

The Scope and Limitations

The study primarily focuses on the perceived vulnerability of inbound tourists on cybercrime in Ghana. Owing to the constraints of time, the study is limited to inbound tourists that visited Ghana between the months of November and January. The research is a cross sectional study and this type of study is characterized by its inability to predict phenomenon overtime. Also, the data collection could not be expanded to cover large respondents. Therefore, it would be beneficial for future researchers to especially assess tourists' cybercrime experiences on a longitudinal study since new forms of cybercrime evolves by the day. Secondly, the study used a non-probabilistic sampling procedure (i.e. accidental sampling) for the survey and, while it does advise that caution should be taken in the generalization of the results, the use of mix method in future research would be preferable to probe further into how inbound tourists got victimized.

Organization of the Thesis

The study is organized into five chapters. Chapter One constitutes the general overview of the study; and contains issues like background of the study, problem statement, research questions guiding the study, aim and objectives of the study, significance of the study, scope and limitations. Chapter Two covers the review of related literature and theoretical concepts underpinning the study, and the conceptual framework used in explaining the subject matter. Chapter Three addresses the research methods which include: the study area, research design, sampling techniques, sample size, sources of data, research instruments, data analysis, ethical considerations, and the problems encountered on the field. Chapter Four focuses on data presentation and discussion of findings from the data gathered from the field. Lastly, Chapter Five provides a summary, conclusions based on the findings, recommendations, and suggestion for future studies.

Operational Definitions

This section presents the operational meanings of the key words that are used in the study. They are explained in ways that communicate the actual meaning as used in the study. The meanings may be different from the usual definition.

Cybercrime*:* this is any criminal activity or crime in which computing devices such as smart phones, laptops and or other forms of ICTs like credit card and its internet/networks/Wi-Fi or applications are the target or the medium through which the act is perpetrated.

Inbound tourists*:* foreigners travelling to Ghana for leisure, business, holiday, and other related purposes for not more than a year and not less than twenty-four hours.

Perceived vulnerability: this is defined as the views of inbound tourists on the attributes or certain peculiar features that make them prone to cybercrime victimization.

Cybercrime experiences: Cyber-victimization is conceptualized as victimization resulting from cyber-criminal behavior. Cyber-victimization also refers to the process of offending others through the use of information and communication technologies.

CHAPTER TWO

LITERATURE REVIEW AND CONCEPTUAL FRAMEWORK

Introduction

This chapter reviews related literature on perceived vulnerability and experiences of inbound tourists on cybercrime in Ghana. The issues covered include the history and origin of cybercrime in Ghana, the concept of cybercrime, factors that influence cybercrime, offenders' motivations for involving in the cybercrime activities, technology and tourism, cybercrime in the tourism industry, the essence of tourists' security and activities that make tourists vulnerable to cybercrime. The chapter is concluded with the theoretical model underpinning the study.

The Concept and Overview of Cybercrime

Various Definitions of Cybercrime

Despite almost forty years of cybercrime incidents, it still does not have a universally accepted definition in literature (Dashora, 2011). Although there are many definitions of cybercrime, the term generally refers to crimes committed through the use of computers and computer networks, but it also includes crimes that do not rely heavily on computers (Britz, 2008). The term cybercrime is also known as "computer crime", "digital crime", "Internet crime", and "high tech crime", and it is commonly understood to include a broad range of criminal activities that use computers, digital devices, and the Internet (Dashora, 2011).

According to Gordon, Hosmer, Siedsma and Rebovich (2003), a uniform definition for cybercrime is very comprehensive since it must cover the different roles a computer may take in the offense, be it the target of the offender, the instrument used to commit the offense, or simply incidental to the crime. Also, the concept of cybercrime comprises unauthorized access to computers and the data stored on them as well as data alteration, and making it inaccessible when needed by the authorized user or owner (Goodman, 2001).

Pati (2003) defined cybercrime as criminal activities or crimes in which computing devices such as smart phones, laptops and or other forms of ICTs like credit cards, the internet and Wi-Fi are the target source. Duggal (2015) considers cybercrime as any criminal activity that uses a computer either as an instrumentality, target or a means for perpetrating further traditional crimes. Duggal grouped cybercrime into three broad categories; crime against individuals (that is the person or his/her property); crime against organization (such as companies, corporations, or government establishment); and crime against society at large.

In the view of Okeshola and Adeta (2013), cybercrime involves committing crime through the internet, it does not necessarily mean it has to happen inside the cyber cafe, one can have his laptop and modem in his house and commit crime. In the Norton Cyber Security Insights Report (2018), cybercrime is defined as one or more of these events; having payment information stolen from your phone, being a victim of identity theft, experiencing credit or debit card fraud, making a purchase online that turned out to be a scam, having an account's password compromised, using someone's private Wi-Fi without permission, gaining unauthorized access to a smart home device, among others.

It could therefore be seen that, cybercrime has been defined in numerous ways by different scholars and authors but in this study, the researcher seeks to use the definition of Pati (2003) which states that, cybercrime is any criminal activity in which computing devices such as smart phones and laptops or other forms of ICTs like credit cards, the internet and Wi-Fi are either the target source or the medium of operation.

The Scope of Cybercrime

According to Gurjar, Baggalli, Breitinger and Fischer (2015), the first published report of cybercrime occurred in the 1960s as also cited in the work of Aidoo, Akotoye and Ayebi-Arthur (2012) that; cases of computer crimes globally, date back to the early 1960s when the first case of cybercrime was reported. Gurjar et al., (2015) explained that, the existence of cybercrime in the 1960 could be true with the fact that, computer existed since 3500 BC in India, China and Japan in Banks and other financial institutions. Since then, there have been countless reports of computer crimes being committed on a daily basis (Kabay, 2008). The first case cited as an instance of the computer fraud involved equity-funding Corporation in the U.S and that was when computer fraud scheme emerged. As technological advancement increased and spread all over the world, so has the number of cybercrime cases increased around the globe (Gurjar et al., 2015).

Globally, the leading state involved in cybercrime is the United States, followed by U.K (Warner, 2011). Within Sub-Saharan African countries like Nigeria, Cameroon and Ghana, especially along the West African coast, there has been a growth in ICT-based businesses and services like internet market and electronic banking services. Unfortunately, the internet has become a doubleedged sword which has raised the specter of new criminal activities arising to exploit internet users. As a result, Nigeria Ghana and Cameroun were spotted to be among the top 10 countries where cybercrime is most prevalent, (Ghana Business News Dec 2nd, 2010) as cited in (Kwablah, 2009).

History and Origin of Cybercrime in Ghana

Media publications stress on the fact that, cybercrime is a relatively new crime that is growing progressively within the borders of Ghana (The Ghanaian Times, 04/06/2012:8). According to an anonymous source within the Criminal Investigating Department, cyber-fraud came into existence in Ghana between the year 1999 and 2000 (Warner, 2011). Within that period, electronically based crimes were mainly related to credit card fraud, which was initially facilitated by bellhops working at the various international hotel chains who would share Western visitors' credit card information with scammers in the country. These Ghanaians would then use the stolen numbers of Western credit cards to purchase goods from the internet, and have them shipped to Ghana.

Duah and Kwabena (2015) asserted that, cyber fraud in Ghana was carried over as a result of the influx of Nigerians into Ghana. Henderson (2007) mentioned that some of Ghana's most prevalent types of cyber fraud such as banking fraud and blackmail are similar to that of Chinese hacking circles, and it is presently viewed that, the same trends and operations of Ghanaian cybercrime are also very common in Nigeria. As a result of these unscrupulous activities on the part of some Ghanaians, Kwablah (2009) revealed that Ghana became the second most frequently blocked location by U.S. online retailers as a result of fake orders from Internet scammers.

However, around 2004, credit card fraud dropped; instead, newer forms of Internet fraud begun to take shape (Anonymous employee of the Ghana Criminal Investigations Department, personal communication) as cited in (Warner, 2011). As a result, three primary types of cyber-fraud were most commonly perpetrated in the country; identity fraud, fake gold dealers and that of estate fraud. With the issue of identity fraud (more specifically identity theft and romance theft or dating scam), Ghanaians were astonishingly the third most frequenting nationality behind Americans and Britons attacks (Ghana and Nigeria: Scammers in E-Harmony, 2011). This came as a result of many Ghanaians contacting Westerners often through social networking sites like Facebook, Internet dating sites like Match.com, eHarmony.com, among others with intentions of duping them.

According to Warner (2009), another form of cybercrime which is locally known as Sakawa is one underreported ground-level aspect of Ghanaian cybercrime gaining root from day to day. In the view of Boateng, Olumide, Isabalija and Budu (2011), fraudsters are locally known as “sakawa” in Ghana. According to Frimpong (2011), the word ‘sakawa’ is corrupted version of the Akan phrase “hye kawa” (to wear a ring). This phrase denotes magical rings that spiritualists mandate fraudsters to wear on their index finger and to be used at all times to press the ‘enter’ key on the keyboard when communicating with potential ‘clients’ or ‘mugu’ (a person about to be defrauded or actually defrauded or still on the hook to be defrauded? The belief is that if the ringed finger is used to execute the command, then all the demands in the email message is infused with a spiritual force that compels the client to accede to all the requests in the mail be it money or other material items.

In the view of Duah and Kwabena (2015), one of the strategies that these fraudsters allegedly use to contact their victims is either through mass-mailing or through a lead. The most popular baits include gold, diamond, lottery and some abandoned money that the client can help recover. The use of fake documents which sometimes originate from genuine sources such as the Office of the President, Attorney General's Department and respectable banks and at times a duplicate website is designed which may look similar to a legitimate one. According to Duah and Kwabena (2015) again, fraudsters scout dating sites and examine profiles of males/females who are interested in relationships. They would then create profiles that match those of their potential 'mugu' (client). They then use photographs either taken from the web or that of a female accomplice. The victim to this type of cybercrime is usually a bored rich old man or someone in the mid-forties. The victim commits to love over the internet with the hope that they will meet their lovers eventually which later lead to duping.

Incidents of Cybercrime in Ghana

General news from Ghanaweb on August (2013) reported that, Ghana was ranked second in Africa after Nigerian in terms of internet scam. Technology analyst John-Osei Seidu told Biztechafrica.com on (July 8, 2014, 2:04 p.m.) that, cybercrime in Ghana is out of control as the government seemed to have run out of ideas as to how best to tackle it. As a result of these, committing more funds to tackle cybercrime has become a problem, including providing adequate logistics to the police to effectively handle this kind of crime which is gradually tarnishing the country's image.

According to the Ministry of Communication, about 82 cybercrimes occur in Ghana every month and that is averagely 1000 crimes a year in Ghana. The study of Coomson (2006) identified credit card fraud as the most prevalent cybercrime in Ghana. The data showed that the search interest for credit cards in Ghana is higher than in any other country. The perpetrators are alleged to be selling stolen credit card numbers as well as using them to order for products from the United States and Europe. Coomson (2006) also reported that they even go online, place orders and then work in partnership with people in the USA or Europe, whose addresses they use and then ask the illegally purchased goods to be delivered to Ghana. These scammers buy or steal credit cards and verification numbers from some hotel employees and cashiers of super markets, either in the country or from abroad (Coomson 2006).

Another worrying form of cybercrime crime is mobile money fraud. The introduction of mobile money has suffered from attempts at defrauding the system by malicious actors (Ursula Owusu stated on Business News on 22nd Oct 2018). Speaking on the climax of the National Cyber Security Awareness month pointed out that, in 2017, one of the telecommunication companies reported it received about 365 complaints of mobile money fraud monthly from its subscribers. Meanwhile, the use of fake IDs for registering SIM cards has slowed down the prosecution of offenders. From Ursula’s presentation also, only 10% of reported fraud cases have been investigated and prosecuted.

In 2014, Issa Sikiti Silva a Ghanaian news reporter in Accra presented that, the police caught six alleged cybercriminals from Nigeria in the old suburb of Adabraka in the capital, Accra, for possessing letterheads of the

Presidency, Interior Ministry, High Court and other state institutions, which they reportedly used to defraud people. Two of these young men - all unemployed graduates - said they owned an online accommodation agency which they use to scam people. Also, on the 20th March 2017, one Seth J. Bokpe in the News reported a case of 30 Cyber fraudsters being arrested at Alhaji Tabora in Accra by the Achimota Mile 7 Police in Accra. The suspects are aged from 21 to 30 and retrieved from their bags were 34 laptops and 48 mobile phones they allegedly used in committing crimes. Out of the 30 guys, only one was a Ghanaian with the remaining being Nigerians residing in the country.

Ennin (2015) conducted a study on cybercrime in Ghana; A study on offenders, victims and the law. The objectives of the study included how victims get lured into cybercrime activities. The investigation revealed that cybercriminals in Ghana engage in different forms of internet crimes such as gold fraud, romance fraud, and online shopping to rip-off their client. The study further highlighted that bogus business proposals, vehicle marked “for sale”, mobile phone lottery, America green card lottery, and rent apartment scams are common internet fraud experienced by victims in Accra. The findings lastly demonstrated that the majority of victims heeded to scammers request without due diligence and some people get lured into internet fraud because of unrealistic profit ventures.

Abem (2013) also conducted a study on cybercrime in Ghana. From the findings, majority of the respondents (72.73%) strongly agreed that cybercrime poses a threat to the country’s reputation and also has negative implications on the country’s economy. Majority of the respondents pointed out that;

unemployment especially among the youth, the quest to get rich quick, gullible foreigners who are greedy on cheap gold deals, lack of strong legislation, lack of commitment of bank staff as well as money transfer operators are major causative factors of cybercrime.

Offenders Motivations for Perpetrating Cybercrime

Just like conventional crime, there are many reasons why cyber-criminals commit cybercrime. Ayofe and Osunade (2009) identified three major reasons why people commit cybercrime which according to them are the chief among them and are; Cybercrimes which are committed for the sake of recognition and is mostly committed by youngsters who want to be noticed and feel among the group of the big and tough guys in the society. Another cause of cybercrime is to make quick money. This group is greed motivated and is career criminals, who tamper with data on the net or system especially, e-commerce, and e-banking data information with the major goal of committing fraud. Thirdly, cybercrime can be committed to fight a cause one thinks he believes in; to cause threat and most often cause damages that affect the recipients adversely.

Furnell (2001) highlighted seven elements of motivation for committing cybercrime which are; challenge, ego, espionage, ideology, mischief, money and revenge. However, Das and Nayak (2013) also identified population growth as a cause of cybercrime and stated that, there exist a positive correlation between the growth in crime and the population of the country. Aside population as a factor, other factors are; the rate of urbanization, migration of population from neighboring places, unemployment, income inequality, computer literacy, among others.

Warner (2011), and Reingold (1999) opined that high rate of unemployment brings about lots of criminal activities, which cybercrime is not exempted. Also, Magele (2005) and Meke (2012) revealed that, poor people are more likely to commit cybercrime than the rich people. But in the view of Boateng et al., (2010), cyber criminals capitalize on system vulnerabilities, ignorance and gullibility on the part of users or potential victims to perpetrate their heinous crimes. Okeshola and Adeta (2013) also added that, parents of today have neglected their rightful roles and parental duties and as such have made most children irresponsible. Although people make their own decision to enter into cybercrime practices, Shehu (2014) believe that, lack of good moral upbringing from guardians and parents are major determinants of their wards future choices.

Just as it is revealed in the studies of Das and Nayak (2013), Hassan, Lass, and Makinde (2012) also in their study identified urbanization as one of the causes of cybercrime Nigeria. They concluded that, urbanization without crime is impossible because an increasing rate of urban population brings about tight competition in search of a better living which in turn makes people involve themselves in all sort of means to survive. Shehu (2014) also identified 'Easiness to Perpetrate' as one other cause of cybercrime. Most especially, Ghana and Nigeria is noted for the influx of second hand laptops amidst its affordability (Hassan et al., 2012) and as result makes people indulge in the act of cybercrime.

Activities that make Tourists' Vulnerable to Cybercrime

The use of Information Communication Technology poses privacy and security concerns to users such as the tourists (Cunningham, Gerlach, & Harper, 2005). Meanwhile those who use smart phones are more vulnerable to these threats/attacks: malware, spyware, botnets, sniffing, automatic data transmission, and device theft (Markelj & Bernik, 2015). Hackers and attackers are not only able to abuse the computer system of the hotels by using different type of phishing email, viruses and stealing guests information but they are also able to attack and take advantage of Wi-Fi in the hotels thereby making guests and the tourists' vulnerable.

Most of the hotels and tourism facilities nowadays offer free Wi-Fi to their guests and all guests will have access to the same network all over the hotel such as lobby, convention center, dining room and all other places within the hotel. According to Noone (2015), hotels' Wi-Fi hackers offer "updates" for software that are famous such as Adobe Reader or Flash Player so that the users like the tourists won't hesitate to update their software meanwhile those updates contain malware that criminals use to get all the usernames, passwords or any other important information from users' computer or smartphone.

IT users such as the tourists are vulnerable to various security threats and attacks especially when they are using tourism facilities such as the hotels. The most common threats include viruses, laptop theft which comes with it associated challenges, spoofing, unauthorized insider and outside attack, and denial of service attacks (Cobanoglu, & Demicco, 2007). According to Mest (2015), the American Hotel & Lodging Association reported that, each minute there are about 480 fake online hotel booking website which are being created which is an amazing place for cyber criminals to take advantage. This implies that, since tourists are noted for making online bookings and reservations, they are vulnerable to online fraud through these fake online booking websites.

According to Shabani (2016), lack of knowledge on cybercrime is the biggest mistake which makes hoteliers and their guests vulnerable to hackers and attackers. Therefore, as long as tourists do not have any idea about how to secure themselves at the destination, hackers and cyber attackers will have more opportunity to take advantage of this issue. Also, in the findings of Shabani (2016), if cyber security in tourism facilities especially with hotels is very low, it makes the hotel very vulnerable to cyber attackers and its implications are also felt by the guests/tourists. Clark (2015) also argued that hotel's property management system if not properly secured could easily be accessed by hackers and attackers to have whatever they want to know about the hotels customers' information and database thereby making the visitors vulnerable to cybercrime.

Factors Influencing Tourists Cybercrime Victimization

Certain background characteristics of inbound tourists' (socio demographics and travel characteristics) predispose them to cybercrime victimization. The influence of age on vulnerability to fraud is one of the best-researched aspects of fraud victimization. Researchers have generally concluded that age is one of main correlates of fraud vulnerability (Button, Nicholls, Kerr & Owen, 2014; Schoepfer & Piquero, 2009). A review by Schoepfer and Piquero (2009) on victimization indicates that, younger individuals are more likely to be targeted and victimized by fraud, this is because they mostly engage in risk-taking activities such as online shopping (Pratt, Holtfreter & Reisig, 2010), and are also more likely to become victims of consumer fraud (Van Wyk & Mason, 2001), than older individuals (Pratt et al., 2010). Middle-aged individuals (those age 45 and under), on the other hand, are found to be more likely to become victims of investment scams (Trahan, Marquart & Mullings, 2005) and Ponzi scams (Ganzini, McFarland, & Bloom, 1990) and older people are more likely to become victims of off-line scams than younger individuals (Ganzini et al., 1990). In terms of gender**,** Boakye (2012) revealed that, males are more likely to be victimized than females in relation to conventional crimes.

Also, the routine activities and self-control (Ngo & Paternoster, 2011; Pratt et al., 2010; Sheng, Holbrook, Kumaraguru, Cranor & Downs, 2010), as well as the degree of computer proficiency and fraud awareness (Pratt et al., 2010) are factors that could influence cyber victimization. For example, older Internet users could be less vulnerable to Internet fraud than younger users because they are less likely to engage in online shopping, but they may be more vulnerable to online dating scams because they are more likely to be visiting online dating sites than younger users (Stephure, Boon, Mackinnon & Deveau, 2009; Valkenburg & Peter, 2007).

According to Grimes, Hough, Mazur and Signorella (2010) also, older Internet users are less likely to have formal computer training provided in employment or educational settings, less aware of potential threats like viruses and phishing, less likely to utilize spyware detectors on their computers, and less likely to alter risky online behaviors to reduce risks of identity fraud and more likely to make online purchases from links provided in spam emails. Regarding the country of residence, there is currently a lack of research comparing the vulnerability of users from different countries to fraud or cyber victimization (Garrett, 2014). But with conventional crime, Boakye (2012) found Asians and Africans to be more likely to be safe than the remaining tourists from other continents.

Regarding the level of education, reviews by Copes, Kerley, Huff, and Kane (2010) and Modic (2012) indicated an influence of formal education on vulnerability to phishing targeting. Education functions as a protective factor by increasing the likelihood of obtaining training in computer security measures, and increasing general computer knowledge (Garrett, 2014). Evidence indicates that educated users would be less likely to respond to phishing emails (Modic, 2012; Sheng et al., 2010). Regarding relationship scams and fraud in general, higher educational attainment appears to be a risk factor for fraud (Copes et al., 2010; Titus, 1999) and identity theft (Pratt et al., 2010). In the views of Pratt et al., (2010), individuals with higher income tend to spend more time online and it is more likely they use the Internet for shopping. Reviews by Button et al., (2009) and Muscat, Graycar and James (2002) cited studies showing that victims of different types of consumer fraud were found to have above-average incomes.

Although the effects of marital status on off-line fraud have been researched more extensively but with cybercrime, married people are more likely to engage in what is considered to be risky online behaviors, such as online shopping (Pratt et al., 2010). Garrett (2014) sees the lack of research on this context as because so many studies of online victimization are undertaken using student samples. Again, awareness of online vulnerabilities may not always lead to a more risk-conscious but it is also associated with an overall lower victimization risk (Sheng et al., 2010; Wright & Marett, 2010), because online security measures provided by third parties such as anti-spam software, online security warnings, are more effective if the users know how to interpret them, or know where to look for them.

The Importance of Technological Advancement in the Tourism Industry

The tourism industry, just like any service industry is primarily high customer contact industry that deals with a great deal of sensitive customer information from reservation details and payment to the collection of other tourists' information. Technology is evolving at a faster pace and effect has made most travellers around the world much more technology-savvy than in the past (AM-reports – Technology in Tourism UNWTO, 2012). Information technology has played a central role in the growth and development of the tourism industry through supporting the internal functions of large operators in the transportation, hotel and food services sectors (Haque & Rahman, 2012).

Developments in search engines, carrying capacity and speed of networks have influenced the number of travellers around the world that use technologies for planning and experiencing their travels (Buhalis & Law, 2008). In order to satisfy tourism demand and survive in the long term, there is no choice but to incorporate technology and enhance the interactivity with the market place, (Haque & Rahman, 2012). Yaun, Gretzel and Fesenmaier (2006) emphasized that, the travel information system has become important link provider between travelers and industry players but it is not out of side effect such as cybercrime (Hasan, Rahman, Abdillah & Omar, 2015).

ICTs enable travellers to access reliable and accurate information as well as to undertake reservations in a fraction of time compared to the cost and inconvenience required by conventional methods (O'Connor, 1999). In the views of Buhalis and Law (2008), ICTs can assist the improvement of the service quality and contribute to higher traveller satisfaction. The development of ICTs and particularly the Internet empowered the "new" tourist who is becoming knowledgeable and is always seeking exceptional value for money and time. Tourists are less interested in following the crowds in packaged tours and much more keen to pursue their own preferences and schedules. This is because, new, experienced, sophisticated, and demanding travellers require interacting with suppliers to satisfy their own specific needs and wishes through the use of; online travel agencies (such as Expedia), search engines and meta-search engines (such as Google and Kayak respectively), destination management systems (such as visitbritain.com), social networking and web 2.0 portals (such as wayn and tripadvisor), price comparison sites (such as kelkoo), individual suppliers and intermediaries sites among others (Buhalis & Law, 2008).

According to Haque and Rahman (2012), the introduction of information technology in the tourism industry has changed its dimensions and resulted in the form of exponential growth. For real time, availability of seats in the aircraft, railways & Volvos and online bookings testify that, IT plays very important role in the tourism and travel industry. Hotels are also using Intrusion Detection System (IDS), interactive TV and Interactive Phone for reservations and other operations. Many software and networking channels have also been developed for travel agencies for activities ranging from bookings to accounting (Haque & Rahman, 2012).

Yaun, Gretzel and Fesenmaier (2006) pointed out that, the Central Reservation Systems (CRSs) and Global Distribution Systems (GDSs); Sabre, Amadeus, Galileo and Worldspan were all developed by airlines and hotel companies to enable travel agencies (and other similar businesses) to access schedule and pricing information and to request reservation for clients.

Travellers search for travel related information, make online air ticket bookings, online room reservations, and other online purchases possible instead of relying on travel agencies to undertake this process for them (Morrison, 2013). The popularity of Internet applications has made most tourism organizations such as hotels, airlines, and travel agencies embraced Internet technologies as part of their marketing and communication strategies (Buhalis & Law, 2008).

Tourists, just like the ordinary individuals regularly utilize their laptops, desktops, tablet computers and smart phones to engage in activities such as communications (Barrett, Steingruebl & Smith, 2011). Social networking sites like Facebook, WhatsApp, Viber, Tango, Instagram and Twitter also allow individuals to stay in touch with friends and family and as well share and exchange ideas around the world, entertainment within 24 hours a day, and with most consumers now even utilizing electronic banking services and credit cards to manage their accounts and paying bills (Anderson, 2010).

The Impacts of Cybercrime on the Tourism Industry

According to Trust wave's 2012 Global Security Report, the hospitality and tourism industry was found to be ranked at the top of the list for data breaches and has remained on top for four consecutive years. Cyber-attackers in the tourism industry can be from both inside and outside the various facilities (Cobanoglu, & Demicco, 2007). Especially in hospitality and tourism firms where turnover rate is very high, the possibility of inside attacks is higher in comparison to other industries (Cobanoglu, & Demicco, 2007). It is also estimated that, security breaches in the hospitality industry are far higher than even the financial services or retail sectors (Yassir & Nayak, 2012). Consequently, some organizations, such as Burger King Corporation, take measures to prevent inside attackers, and provide infrastructure to ensure only a single sign-on by an employee (Liddle, 2003).

The use of Wi-Fi in most tourism sectors such as hotels, airports, theme parks, and the rest also has the potential to open doors to cyber criminals; allow unauthorized entry of privacy hackers and revealing guests' or visitors confidential/personal information (Nayak, 2016). Crime dynamics and victimization are not alien to the set of changes wrought by the digital era (Salvador, 2015). Many tourists seem to travel just for the experience and enjoyment of shopping (Timothy & Butler, 1995). Therefore, crimes are evident since shoppers sometimes make payments with credit cards and so their financial information could be stolen during transactions which can lead to personal identity theft (Pehlivan, Yϋksel & Yϋksel, 2007).

Nayak (2016) conducted a study on the impacts of cybercrime on the tourism industry. The study revealed that, the global annual loss incurred accounted to be $1200,000 as the financial loss which Airline/Shipping industry incurred due to cyber-attacks. The cost of recovery (the cost which was recovered by the Airline industry) was $263,410 (which average cost per cyber-attack was $800). Also, the global annual lost incurred by the hospitality and tourism industry worldwide was $614,000 due to cyber-attacks and the cost of recovery was $70096 (the cost which was recovered by the telecom industry) with an average cost per cyber-attack as $800.

Lavelle (2016) finding revealed that, the Mandarin Oriental Hotels experienced data breach. The breach was a result of credit and debit card information of those customers who used spa, beverages, guest rooms, dining room and other product and services. Finally, on October 2015, Trump Hotel Collection confirmed the data breach and it alarmed the customers who used their credit card in the hotels between May 19, 2014 and June 2, 2015. This data breach happened in several Trump locations such as SoHo New York, Trump International Hotel and Tower Las Vegas, Trump International Waikiki and Trump International Chicago (Petri, 2015).

Perceived vulnerabilities to cybercrime

Kamruzzaman, Islam, Islam, Hossain and Hakim (2016) findings revealed that, the most vulnerable respondents of cybercrime were between ages 19 to 21 years with 66.1 percent being males 46.61 percent being females. About 60.16 percent professed to be vulnerable to cybercrime by Internet fraud and a little over three quarter (78.81%) agreed that it is social media that increases their level of vulnerability whereas 72.03 percent felt unsafe in cyber space.

Dimc and Dobovsek (2010) also conducted a study on the perceptions of cybercrime in Slovenia. The study focused on the perception of cybercrime among the general public, as well as the members of the law enforcement agencies. Notable among the objectives of the study was to determine the perceptions of respondents' safety on the internet. The finding revealed that, more than three quarters of the interviewees (80 %) feel safe in the cyberspace and therefore do not perceive themselves to be vulnerable to cybercrime while only 20 percent of them actually expressed the opinion that they do not feel safe online due to their activeness on online social networks such as Facebook, twitter, netlog, MySpace among others.

Experiences of Cybercrime

Okeshola and Adeta (2013) conducted a study on the causes and consequences of cybercrime in Tertiary Institutions in Nigeria. From the findings, majority of the respondents were of the view that hacking (85%) and credit card frauds (78%) are the common type of cybercrime in Zaria - Nigeria. However, malicious program/virus dissemination (32%) and cyber stalking (27%) are other types of cybercrime that obtained lower frequencies.

Whitty and Buchanan (2012) also conducted a study on online romance scam as a type of cybercrime. With a total sample of 2028 British adults aged 18 years and above, 902 were men and the remaining 1126 were women. The researchers utilized the services of YouGov (www.yougov. co.uk), a professional research and consulting organization that have panels of individuals who have agreed to take part in online surveys. Overall it was found that 0.65 percent of the sample had been scammed. Moreover, 2.28 percent of the sample claimed they personally knew someone who had been scammed.

Kamruzzaman et al., (2016) did a study on the plight of youth perception on cybercrime in South Asia among youth, using purposive sampling method with a sum of 118 respondents. Most of respondents were between ages 19 to 21 years with (66.10%) being males and (46.61%) females. The findings revealed that, most respondents (82.20%) were affected by virus attack.

The study of Dimc and Dobovsek (2010), focused on the perception of cybercrime in Slovenia. The majority of the interviewees (81%) have had an experience with cybercrime with malicious programming code infecting their computer systems. Also, 50% of the interviewees have had an experience with an attempt of online fraud. Almost all interviewees, with the exception of one, although had encounter with an attempt of cybercrime but never experienced any monetary loses. Despite the increasing number of cybercrime cases all over the world and also in Slovenia, the majority of interviewees (80 %) stated that they feel safe in the cyberspace.

Shabani (2016) undertook a study of cyber security in the hospitality industry, threats and countermeasures in Reno, Nevada. The findings revealed that, out of the 10 hotel guests interviewed, only one said he has experienced a fake website while he was booking a hotel two years ago and he did not recognize the issue until the time he went for check-in and the front desk employee told him that his name is not in the list. He also mentioned that the front desk employee already knew about the fake website since they had another customer who had complained or reported the same thing. One of the respondents also mentioned that after coming back from his trip, he observed some unusual credit card activities, so he called the bank and informed them and get his money refunded.

Preventive Strategies to Cyber-Crime

Within the context of conventional crime, individuals try to save their houses, cars, offices and other personal properties with technical checks such as CCTV and Alarms. Similarly, people can protect themselves in cyberspace with the help of little technical education and common sense (Avais, Wassan, Narejo & Khan, 2014). Chen, Paik and McCabe (2014) explored internet security perceptions and practices in urban Ghana. The respondents were; Junior secondary school or less 13 (7%), Senior secondary school 53 (28%) Polytechnic or post-secondary teacher training 37 (20%) and University 63

(34%) Graduate school 20 (11%). Regarding their individual security measures on their technology use and internet, over 76% expressed the use of password as an effective tool for cybercrime prevention. From the findings of Shabani (2017) also, out of the 50 hotel guests interviewed on their cybercrime coping mechanisms, 27 added that, they use strong passwords to secure their data and IT gadgets.

In the view of Nayak (2016), a number of tactics and techniques can be used to prevent or reduce cybercrime activities, including the legal system and existing and emerging technologies. All the security breaches such as virus infections, identity theft and hacking are the direct cause of carelessness and lack of knowledge and action on the part of users (Ten, Lui & Manimaran, 2008). A high level of awareness about information security and cybercrime issues amongst users at their homes, workplaces, among others is of importance. According to Thompson (1979), passwords remain one of the major preventive mechanisms deploy by individuals in preventing cybercrime. Merritt (2007) has also contributed to the various strategies that can be adopted to avoid being attacked by cybercriminals. In the view of Merritt, one must guard private data by being careful with personal information on Social Security numbers, account data, and passwords. Also review bank, investment, and even online auction payment accounts diligently. Sign up for fraud alerts on credit cards and check statements carefully each month. Manage credit report well and make sure no one uses his/her hard-earned money for their personal gain. Be cautious about online transactions, especially on neighborhood trading sites and auction sites.

Alpna and Malhotra (2016) also revealed these strategies as means of preventing cyber victimization;

- Use strong passwords by; using separate ID/password combinations for different accounts, Avoiding writing them down, Making the passwords more complicated by combining letters, numbers, and special characters, Changing passwords on a regular basis, Not using passwords that contain names, birthdays and phone numbers, Not sharing passwords across multiple services i.e. same password for Gmail, Credit Cards, Work, and Twitter, Keeping password is in one's brain and, Not revealing password to anyone, including people from support, customer service or even the helpdesk.
- These notwithstanding, enable firewalls, secure wireless network, protect e-identity, and lastly, be too vigilant to be scammed.

Also, the study of Avais, Wassan, Narejo and Khan, (2014) revealed that, 61% respondents were aware regarding safety measures or self-protection tools for cybercrime. The preventive measures provided by the respondents included; internet filtering, block obnoxious person, locked personal walls, albums or friend lists.

Theoretical Framework

Theories of Cybercrime

A number of theories have been suggested in the studies of cybercrime. Notable among them include Space Transition Theory, Routines Activities theory and Lifestyle Exposure Theory. According to Leukfeldt and Yar (2016), there seems to be no consensus about the applicability of the theories of conventional crimes such as the Routine Activity Theory (RAT) in cybercrime. In this regard, there are two schools of thought on the use of crime theories in cybercrime; the transformationists and the continuists. To the "transformationists", cybercrime is a novel phenomenon by virtue of the new space and form within which it happens. To the "continuists" it is simply a case of "a new wine in an old bottle." The first group pleads for the development of new criminological theories, while the latter group argues existing theories, like RAT, can be used.

One of the basic tenets among some of the crime theories like RAT and Lifestyle Exposure Theory holds that every crime can be explained by three major factors: motivation, opportunity, and the absence of a capable guardian. This explanation can apply to an individual incident as well as to long-term trends, so as it explains conventional "street" crime and it is equally applicable to crime in cyberspace (Grabosky, 2001). Thus far, Yar (2005) concluded that the virtual and terrestrial organization of the criminal event are homologous, and hence can be adequately analyzed using RAT or similar situational theories. This thesis is underpinned by the Routine Activity Theory (Cohen & Felson, 1979), Lifestyle Exposure Theory (LET) (Hindelang, Gottfredson, & Garofalo, 1978) and Space Transition Theory (STT) (Jaishankar, 2008). Meanwhile, the fundamental theory for the study is the Routine Activities theory. This is because, the LET and STT all explains the study to some points. They do not possess all the elements which inform the study but RAT does.

Space Transition Theory

This theory views the emergence of cyber space as a new locus of criminal activity and, explains the causation of crimes in the cyber space. Space transition theory was developed in 2008 by Jaishankar and posited the need for a separate theory of cybercrimes because the general theoretical explanations were found to be inadequate as an overall explanation for the phenomenon in the electronic society. In view of this, he propounded the Space Transition

Theory and argued that people behave differently when they move from one space to another.

The various propositions of the theory are;

1. Persons who due to their status and position cannot commit crimes in physical space have tendency to commit crime in cyberspace.

2. Due to lack of deterrence factor, flexibility in identity factor, cyberspace provides the choice to offender to commit Cybercrime,

3. In Cyberspace, behavior of offender is likely to be imported to physical space.

4. Intermittent ventures of offenders in to the cyberspace and the dynamic spatio-temporal nature of cyberspace provide the chance to escape.

5. (A). Cyberspace may lead to unite strangers in physical space to commit crimes. (B). A group of people having common purpose or interest in Physical space are likely to unite to commit crimes in cyberspace.

6. Persons belonging to closed society are more likely to commit crimes than belonging to open society in cyber space.

7. Norms and values of both cyber and physical space may lead to cybercrime.

The theory explains the nature of the behavior of the persons who bring out their conforming and non- conforming behavior in the physical space to the cyber space. This new theory appears to contain several propositions that seem to explain certain cyber-related behaviors and the theory will likely be empirically tested in the future. Holt, Bossler and Spellar, (2015, p. 309 and 313) feels that: "…Space transition theory is one of the few theories created specifically to address cybercrime. Danqua and Longe (2011) tested the Space Transition Theory in Ghana. "They found that Space Transition Theory is more applicable in cyber-trespassing, cyber-deception and theft, and cyberpornography than cyber-violence (Kethineni, Cao & Dodge, 2017, p. 7). Also, Kethineni, Cao and Dodge (2017, pp. 13-14) tested the space transition theory in their study and found some support. In particular, the theory's propositions like identify flexibility, dissociative anonymity, easy online association, and lack of deterrence bring more and more traditional criminals to the Internet. Also, the notion that when there is a conflict between the norms and values of physical space, and the norms and values of cyberspace offenders choose cyberspace has been supported in this study.

Routine Activities Theory (RAT)

The Routine Activities Theory (RAT) has been chosen to provide a theoretical basis for this study. This is the most common theoretical basis for most criminal victimization studies. This theory was propounded by Cohen and Felson, (1979). The theory posits that there are three elements of direct contact predatory crime: A potential or likely offender; someone who is motivated to commit crimes, suitable targets; the presence of things that are valued and that can be transported fairly easily and absence of capable guardians; people to prevent the criminal activity. If one or more of these three necessary elements are absent, the chance of a crime occurring is decreased. This theory proposes that crime occurs during every-day routines in normal life when a suitable target is in the presence of a motivated offender and is without a capable guardian (Cohen & Felson 1979).

Yar (2005) offered a theoretical reflection on RAT's capacity to explain patterns of cybercrime. He proceeds by, first, considering each of the core elements of RAT's schema of the criminogenic situation (motivated offenders, suitable targets, and absence of capable guardians) testing them in terms of their applicability to the on-line environment. With respect to motivated offenders, these would include the various fraudsters, hackers, pirates, stalkers, and so on. Similarly, there are numerous targets which are suitable for predation and these include proprietary data, personal information, on-line payment and purchasing services, as well as computer systems themselves that may be compromised and disrupted by unauthorized intrusion and interference. Lastly, the term 'capable guardian' is used widely; it may include the owner of the property (in the context of phishing, the account holder), law enforcement, Computer Emergency Response Teams (CERTs), banks and financial institutions, or any other individual or agency that has the potential to discourage offenders (Yar 2005). Capable guardians may take a variety of forms, including network administrators, forum moderators, users and peers, range of automated protections such as firewalls, virtual private networks, anti-virus and anti-intrusion software, passwords or security codes, ID authentication and access management systems among others (Williams, 2015).

According to Leukfeldt and Yar (2016), it is difficult to assess the value of RAT in explaining cybercrime. The reason being that, studies focus on different types of crime: ranging from computer viruses to stalking and fraud. Needless to say, these crimes are different in nature and the usability of RAT will therefore be variable also. However, studies focusing on the same type of crime (e.g., malware or fraud) also show different outcomes. RAT's applicability on cybercrimes are nevertheless subject to a number of limitations; these include the reliance on a limited sampling set (such as college students—

Marcum 2008), limited sample size (Choi, 2008), and the focus on a single form of cybercrime such as malware infection (Bossler & Holt, 2009).

For instance, Bossler and Holt (2009) investigated victimization by malware among college students (N = 570). The authors included both on-line activities such as shopping, chatting, and banking and guardianship (computer skills, anti-virus, and deviant peers). They concluded that most routine activities on the computer, as well as personal and physical guardianship, are not correlated with data loss from malware victimization.

Application of RAT Concepts in an Online Environment

The current study looked into different forms of cybercrime victimization inbound tourists might have suffered (computer viruses, phishing, fraud etc). Three parts of RAT were included in the study: visibility (tourists online activities that may expose them to potential fraudsters such as chatting, online shopping, online booking, credit card use, etc), accessibility (making friends with strangers online, providing information), and guardianship (the use of security software and other online practices).

According to Longe, Ngwa, Wada, Mbarika, and Kvasny (2009), the convergence of potential victims and potential offenders in digital space does not require their simultaneous presence in any particular location unlike the offline crime; offenders can simply collect information about potential targets remotely through phishing, spamming, or by buying their information in the online underground marketplaces. This gives room for unlimited number of victim's data the offenders can reuse once harvested, for an unlimited amount of time, as long as the channel by which the target receives information (e.g., a particular email account) remains active. This suggests that it might be more accurate to say the likelihood of online fraud victimization depends on the offenders' ability to access the target through some channel of communication, whether simultaneously shared or not (Garrett, 2014).

Since there are no physical attributes to provide visual or contextual indicators to the identities of other users in cyberspace, a user's online activities (e.g., making particular online purchases, the use of credit card, emails, visiting topic specific Internet chatrooms, etc) play an oversized role in the process of target selection. These actions serve as clues to the potential offenders to indicate which targets are accessible and attractive (Holt & Bossler, 2008; Pratt et al., 2010).

Lifestyle-Exposure Theory (LET)

Lifestyle exposure theory (LET) emphasizes the role of an active victim suggesting that it is the victim's actions that trigger the victimization mechanism (Meier & Miethe, 1993). Hindelang, Gottfredson, and Garofalo (1978) propounded the Lifestyle Exposure Theory and it states that an individual's everyday lifestyle, i.e. individuals' routine activities, influence the amount of exposure to places and times where there is a higher risk of victimization. This criminology theory may provide a suitable framework for the study of the victim-sided factors that increase the risk of cyber victimization (CV). According to the theory, the victim's risky lifestyle is determined by situational factors (exposure to motivated offenders, target attractiveness, and capable guardianship), as well as demographic characteristics. Lifestyle exposure theory suggests that demographic differences in victim risks are attributed to differences in the personal lifestyles of victims. Lifestyles may be diverse based on the level that each individual can adapt to his role expectations (Meier & Miethe, 1993)

The theory states that lifestyles are routine, that the risk of victimization is not differentially exposed, and that the relationships between demographic characteristics and personal victimization can be attributed to lifestyle differences (Hindelang, Gottfredson, & Garofalo, 1978). In other words, if an individual engages in risky lifestyle behaviors, they are more likely to experience victimization than an individual who avoids risky behavior. This theory purports that individuals are targeted based on their lifestyle choices, and that these lifestyle choices expose them to offenders and into situations in which crimes may be committed. There are two major tenants of lifestyle-exposure theory which are the ***individual's vocational and leisure activities***. These activities will include concepts such as social interaction and social activities such as work, school, and leisure activities.

Examples of some lifestyle choices indicated by this theory include going out at night alone, living in "bad" parts of town, associating with known felons, being promiscuous, excessive alcohol use, and doing drugs. In addition to theorizing that victimization is not random, but rather a part of the lifestyle the victims pursues, the lifestyle theory cites research that victims ‘‘share personality’’ and certain behaviors may contribute to their victimization since they cause the individual to put themselves at higher risk for victimization than their more conservative lifestyle counterparts. Linking the lifestyle theory to cybercrime vulnerabilities and experiences, certain reckless online behaviors of some tourists such as visiting online dating sites, frequents online transactions, making friends with unknown people online among others make users contribute to their own victimization.

Conceptual Framework

After a thorough review of literature, the study adopted the Routines Activities Theory (Cohen & Felson, 1979). This theory was selected because it looks at online capable guardianship, a suitable target and motivated offender. The theory posits that crime occurs during every-day online routines in normal life when a suitable target is in the presence of a motivated offender in the absence of a capable guardianship (Cohen & Felson 1979). Further modifications were made to include some socio-demographic variables (continents of origin, sex, age, level of education and marital status) and travel characteristics (travel status, frequency of visit, purpose of visit and information source). These variables were added because of the assumption that there could be some differences in visitors' evaluation of experiences based on these background characteristics.

The main idea emphasized by the conceptual framework is that, demographic factors, travel characteristics and respondents awareness of cybercrime have influence on respondents perceived vulnerability, respondents routine online activities, personal online guardianship and victimization. Thus, a particular tourist age, gender, marital status, education, income, continent of origin, awareness, purpose of visit and frequency of visit will influence his/her perceived vulnerability, victimization, routine online activities and online preventive strategies in a way which may be different from how another tourist will interact with these concepts with respect to the same characteristics.

The framework also proposes that, the routine online activities undertaken by tourist have influence on his or her perceived vulnerability, preventive strategies (online guardianship) as well as their victimization. Moreover, the perceived vulnerability of respondents can influence respondents' routine online activities, inform their choice of preventive strategies or directly influence respondents experiences of cybercrime (victimization) in the absence of capable guardianship (intervening variable). Online preventive strategy (capable guardianship) becomes an intervening variable between online routine activities and cybercrime victimization. This implies that, victimization is not likely to occur if there is the practice of online preventive strategies. Lastly, the kind of preventive strategies adopted by tourists could also influence how they will perceive cybercrime.

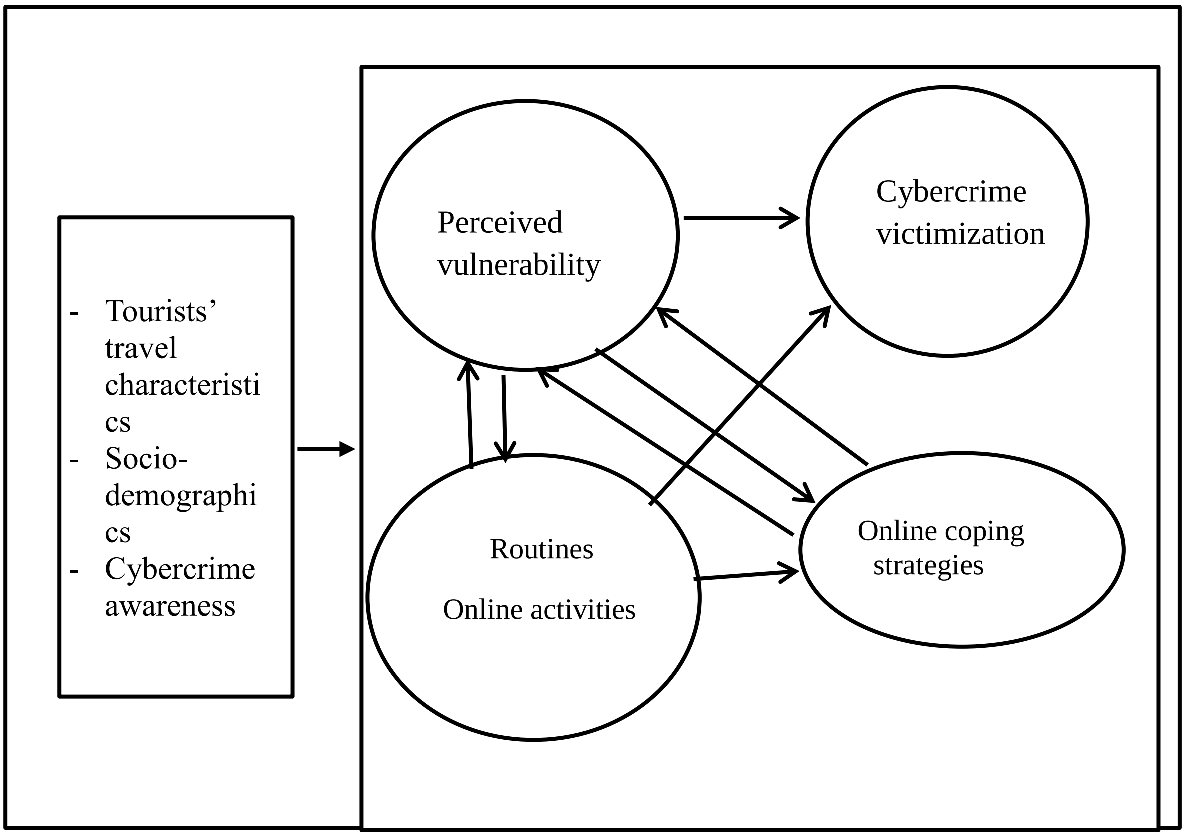

Figure 1: Proposed Conceptual Framework, Authors own Construct.

Sources: adapted from (Cohen and Felson, 1979)

Chapter Summary

The chapter reviewed related literature on the scope and types of cybercrime, the history and origin of cybercrime in Ghana, the importance of security in the tourism industry, perceived vulnerability and experiences of cybercrime as well as the preventive mechanisms to cybercrime. Both theoretical and conceptual underpinnings of the concepts were reviewed. Specifically, theories covered were the Space Transition Theory, Lifestyle Exposure Theory and Routine Activity Theory. Finally, with the RAT being the fundamental theory for this study, a conceptual framework was developed from its various concepts.

CHAPTER THREE

RESEARCH METHODS

Introduction

The chapter presents the methods used in conducting the study. It captures research philosophy and analysis including profile of the study area, research design, sources of data, the target population, sample size and sampling technique, research instrument, data collection procedure, problems encountered on the field, data processing and analytical tools used, and ethical consideration.

Profile of the Study Area

The Republic of Ghana is situated on the Gulf of Guinea and the Atlantic Ocean in West Africa between latitudes 4.5^{o} N and 11^{o}. It is bordered by Togo to the east, Burkina Faso to the north, and Ivory Coast to the west. With a land mass of 238,533 square kilometres, it has a population of 27 million, representing over a hundred ethnic groups and several indigenous languages. English is the official language and Twi is the most widely spoken local language. Ghana is one of the countries that have adopted tourism as an engine of growth and economic development in the West African sub-region since the 1980s. As a developing destination, the contribution of the travel and tourism industry to Ghana's GDP was 12,573.3 ($ 2,864.1) which represents 6.2% of the GDP in 2017 (WTTC, 2018). Ghana is the world's second largest cocoa producer, Africa's second biggest gold miner, and oil producer (Ayeh, 2015). There exist a wide array of tourism offering which the country pride itself with including the Forts and Castles, Beaches, the Kakum National Park, Waterfalls, Crocodile Ponds, Cultural Centers, Mountains and Festivals.

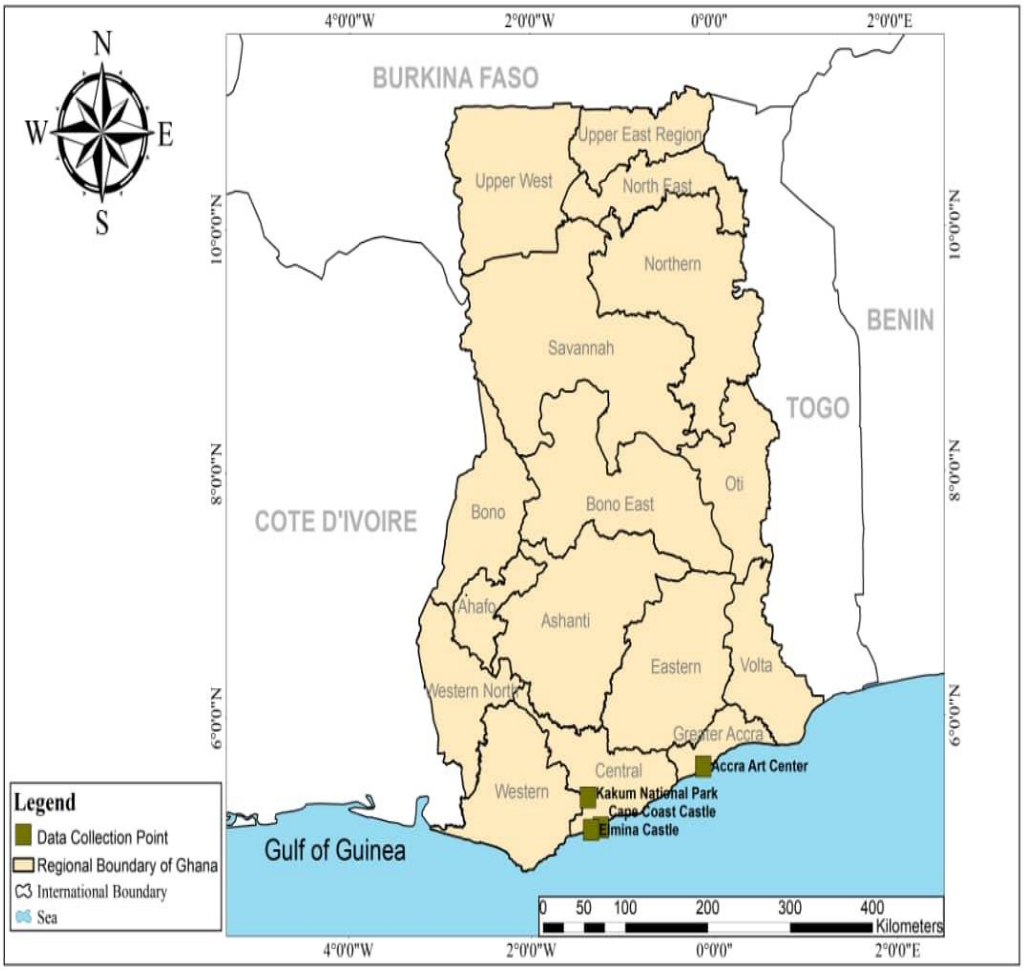

Figure 2: Map of the Study Area and the Location of data Collection Point.

Source: Department of Geography and Regional Planning (2019)

Ghana is one of the promising tourism destinations in sub-Saharan African that endears itself to various types of travelers from different continents (Dayour, 2013; Adam, 2015). The adoption and use of information and communication technologies (ICT) is on the increase across Africa compared to some decades ago (ITU, 2008). This has facilitated globalization and tourism development through publicity, marketing, bookings, online shopping and banking, communications among others. The ICT is a double edge sword and so its adoption has also simultaneously raised the specter of new criminal activities in Ghana which has gained global attention; the media publication where Ghana was ranked seventh in terms of cyber fraud, out of ten countries identified in the world and second in Africa is alarming, (Daily Graphic, 15/04/13, Page 7). According to Dayour et al., (2019) Ghana is characterized by ICT security issues and other physical-safety related issues.

Greater Accra and central region were chosen as destinations for data collection based on the regions peculiar strengths. For instance, Accra is the Capital of Ghana and also the Greater Accra region's tourist hub, the only city with the known international airport, sporting a wide variety of tourist receptive facilities like hotels, food and beverages and transportation, monuments, museums and nightclubs. Another reason being that, irrespective of which part of the country a tourist visits, he or she will surely finalize his journey at Accra for departure. Central region also "as described as the heart-beat of tourism in Ghana" have unique attractions such as the Kakum National Park and the Castles which is continually visited by inbound tourists. Thus, the choice of Accra and the central region as data collection areas will assist the researcher to obtain information from different international tourists with varied experiences from different parts of the country.

Study Design

This study adopted cross-sectional study design. The choice of this design helps the researcher to focus on the unique segment of the tourists rather than the whole population and also obtain an overall picture as it stands at the time of the study (Kumar 2005, p. 23) unlike the longitudinal design. Also, its adoption is less time consuming and relatively simple since it allows one time investigation. This design is also deemed suitable for this study which seeks to do a one-time evaluation (thus, because of the limited time at the researcher's disposal to complete the study) of perceived vulnerability and experiences of inbound tourists on cybercrime in Ghana.

Research Philosophy

This study is grounded by the positivist paradigm of exploring social reality. Positivism is of the view that, the goal of knowledge is to provide a depiction of a particular situation that people have been through whereby the outcomes can be observed and measured. According to Walsham (1995) the positivist position maintains that, scientific knowledge consists of facts and so if the research study consists of a stable and unchanging reality, then the researcher can adopt an 'objectivist' perspective. Based on this, positivism is deemed appropriate since the study seeks to uncover the real experiences of tourists on cybercrime as well as their perceived vulnerabilities to cybercrime. Another notable reason for the choice of positivism is that, the theoretical underpinning of quantitative methodology is positivism. Though there is strong anecdotal information, not much is empirically known about the extent of tourist victimization on cybercrime or the views of tourists about their perceived vulnerability in Ghana. An exploratory design, therefore, offers greater baseline insight to the nature of the phenomenon (in Ghana) and provides a platform for subsequent studies which can then adopt an experimental outlay (Neuman, 2007).

Data and Sources

The study made use of both primary and secondary data. Primary data was obtained from international tourists who visited Ghana and used for the analyses of this study. The data included their perceived vulnerability on cybercrime in Ghana, how their perceived vulnerability on cybercrime influences their travel decisions, their experiences of cybercrime and preventive mechanisms. There is no information that would assist the researcher in addressing all these specific issues (secondary data), hence the need for gathering primary data. Aside the primary data, other secondary information was also sourced from journals, internet, books, media reports and other published materials especially with the development of background and the review of literature. Also, information on tourists' arrivals was obtained from GTA. This assisted in estimating the sample size for the study.

Target Population

The target population for the study comprised international tourists that visited Ghana from November 2018 to January 2019 during instruments distribution, excluding tourists below 18 years. It included only tourists who could read and write the English language. The study excluded children because the researcher assumed that since these children always travel with their parents/guardians and so their decisions and assessment about a phenomenon are mostly influenced by their parents/guardians.

Sample Size and Frame

The sample size for the study 400 international tourists, this was determined using the formula proposed by Yamane (1967). The formula is:

$$n = \frac{N}{1+Ne^2}$$

Where:

n = desired sample size

N = total population

e = the margin of error set at 5% (standard value = 0.05)

According to GTA, the tourism statistics 2014 has it that, the tourists' arrival within that year 2014 was estimated to be one million and ninety-three thousand (1,093,000).

Substituting the values into the formula,

$$n = \frac{1093000}{1 + (1093000) \text{ x } (0.05)^2}$$

$$\mathbf{n} = \frac{1093000}{1 + 2732.5}$$

$$\mathbf{n} = \frac{1093000}{2733.5}$$

$$\mathbf{n} = 399.85$$

Therefore, n = 400 tourists.

Sampling Technique

Data was collected from international tourists in Accra Art Center, Kakum National Park, Hans Cottage Botel and the Cape Coast and Elmina castle. Accidental or convenient sampling technique was used to select the tourists who participated in the study. Thus, this technique was deemed appropriate for the study because the researcher administered questionnaires to only tourists the researcher chanced on at the time of data collection. That is, tourists who were readily available and willing to partake in the exercise in terms of convenient, accessibility and proximity. The choice of such sampling technique is not new to these types of studies since it has been employed in many studies of this nature (George, 2003; Boakye, 2012). For the tourists, the choice of the accidental sampling method is informed mainly by their transient nature making it difficult to acquire a fixed sampling frame which is the basis for probability-type sampling techniques. Also, there is no sampling frame available for all international tourists which would allow the researcher to select specifically who should be included in the study, hence accidental sampling remains the best option.

Data Collection Instrument

Questionnaires were used to gather data for this study. It was designed in English language. The basic assumption for the choice of English language is that, since the official language of Ghana is English, most inbound tourists who visit Ghana will be fluent in both written and oral. Also, other studies (e.g. Adam, 2015; Boakye, 2012; Amissah, 2013; Dayour, 2013) on international tourists in Ghana made use of English Language in the design and administration of questionnaires. For this matter, inbound tourists who were not literate in English language were not included in the study. A total of 400 questionnaires were used in gathering information from the respondents. The use of this type of data collection instrument became appropriate for the study because of its unique characteristics. For instance, according to De Vaus (2002), a questionnaire is used to collect original data of information from a sample. Moreover, it is also characterized by; high response rate and wider coverage, less time and energy to administer and the possibility of anonymity (is higher because subjects' names will not be required on it). These advantages notwithstanding, questionnaires also have weaknesses. For example, there is the question of ‘‘validity’’ and ‘‘accuracy’’ because the subjects might not reflect their true opinions but might answer what they think will please the researcher, and so valuable information may be lost as answers are usually brief (Burns & Grove 1993).

The instrument consisted of five sections. The first part of the questionnaire (section A) focused on the perceived vulnerabilities of inbound tourists on cybercrime in Ghana. Thus, it solicited respondents’ views through closed ended questions, open ended and multiple-choice questions. The next part (section B) deals with how tourists perceived vulnerability influence their travel decisions. With this also, multiple choice questions were provided for the respondents to choose from and as well, open ended questions were also provided which gave room for respondents to express their opinions to the questions provided them.

Section C captured tourists’ actual experiences of cybercrime in Ghana. In this section, respondents were offered questions of close ended, open ended and multiple choices. Section D covered tourists’ preventive mechanisms of cybercrime and the last section talked about the socio-demographic; it explored the profile of the respondents concerning their age, sex, level of education, occupation, religion and marital status and, tourists’ travel characteristics.

Pre-Testing of Instrument

Pre-testing is undertaken to ensure the validity and feasibility of the data collection instrument. Also, another vital reason for pre-testing is to determine the reliability of the instrument. Thus, to check and see if the findings will assist the researcher in realizing the stated objectives. A pre-test was carried out from the 18th of October to 22nd, 2018 at the Kakum National Park in Abrafo Odumasi. A total of 40 respondents were used in order to ensure clarity of the questions as well as the content validity of the instruments for the data collection of the actual work. Kakum National Park was chosen primarily because of accessibility. Kakum National Park was also included in the areas of data collection but because tourists are transient in nature, there is no way the same tourists who took part in the pre-test survey will be included in the actual fieldwork. From the pre-tested instruments, it was realized that, some questions needed to be rephrased or totally removed as a result of reasons such as; ambiguity, double barrel, complexity, among others. For instance, the pre-tested instruments contained a scale type questions on perceived vulnerability which respondents were made to tick based on their level of agreement. From the answers provided in the open-ended questions, the researcher realized that both the scale type and the open-ended questions yielded almost same results and so the scale type had to be deleted. Moreso, the pre-test also enabled the researcher to assess or examined the field assistant whose assistance will be needed in the actual study. That is, it provided the room for training and familiarizing themselves with the experiences required in data collection exercise.

Training of Field Assistants

One past student of the department of Geography and two community tour guides of Kakum National Park who are also past students of the Department of Hospitality and Tourism Management were recruited as field assistants. The choice of these people was based on their past experiences on data collection. A two-day training exercise was organized for them in order to abreast them with the overall objective and sub-objectives of the study. Afterwards, they were taken through the instrument to critically understand the content to the extent where they can as well explain everything vividly to the tourists. Lastly, the field assistants were also asked to practice the act of data collection among themselves with the inclusion of the researcher. They were also asked to adhere to ethical issues and consideration.

Fieldwork Challenges

The main fieldwork lasted two months, from November 1 to January 1, 2019 and was supported by three field assistants. A total of 400 questionnaires were distributed to the inbound tourists. However, after the field work, a total of 370 were deemed or found useful for analysis representing a total of 92.5 percent response rate.

As it has always been the case in most surveys, the major challenge of the study was the fact that the success of the research depended more on the willingness of respondents to cooperate with the researcher and provide detailed responses. However, the following challenges were encountered; first and foremost, there was the unwillingness of the visitors to participate in the study due to language barriers of visitors who could not communicate in English. Some respondents refused to partake with the view that, they came to have pleasurable time for themselves and not anything else. Some actually took the instrument but refused to fill. With this challenge, the researcher had to extend the proposed duration of the fieldwork from one month two weeks, to two months since the needed instrument for the study could not be obtained within that period.

Also, some visitors felt reluctant to partake due to lack of time on their side which resulted mostly in incomplete instrument and visitors' inability to properly provide the information required. The nature of the tour of the visitors also prevented most tourists from participating in the survey due to the strenuous nature of the tour. Most tourists hurried back into their buses to catch up with time while others stayed up busily chatting or refreshing. The researcher also made sure that, the collected instruments were read through on daily basis in order to eliminate the uncompleted ones. This was done on daily bases until the desired number of completed questionnaire was reached.

Data Analysis and Presentation

The Statistical Package for the Social Sciences (SPSS), version 21, was used to analyze the data from the field. Prior to the data entry, the completed instruments obtained from the field were first cleaned in order to do away with incomplete and unanswered questionnaires. The questionnaires were therefore coded into the computer; both descriptive and inferential statistics were used in the analysis. In relation to descriptive statistics, frequencies and percentages were employed to present the background characteristics and travel characteristics of respondents. The findings were presented in the form of tables, charts and figures. Lastly, chi-square test of independence was used to explore the relationship between tourists' background characteristics and perceived vulnerability, and to examine the relation between tourists' victimization against their socio demographics and travel characteristics.

Ethical Issues

All ethical issues such as informed consent, anonymity, and confidentiality were adhered to. Kumekpor (2002) clearly emphasized that the most important elements in the research enterprise are the respondents, and so everything must be done to alleviate their fears and anxiety. Bryman (2008) also warned that the fundamental ethical principles of social research are: never coerce anyone into participating; participation must be voluntary at all times. Permission alone is not enough; people need to know what they are being asked to participate so that they can make informed decisions.

Having been embedded with these great scholars' thoughts, an introductory letter was obtained from the Tourism Department, University of Cape Coast, to officially authenticate the researcher's right to data collection in various attraction sites. In addition, an ethical clearance was obtained from University of Cape Coast Institutional Review Board (IRB) whose primary goal is protecting research participants from physical or psychological harm. Moreover, privacy, anonymity informed consent, and confidentiality of the participants were adhered to by the researcher to protect the respondents' identity.

Summary

This chapter discussed the methodology used in carrying out the study. It considered many issues among which are the description of the study area and the study design. Other issues include the target population, sources of data, sample size and the sampling procedure, and the research instrument. The chapter was concluded with issues pertaining to pre-testing, training of field assistants, ethical issues, challenges encountered during the fieldwork and data processing and analysis of the pre-tested instruments.

CHAPTER FOUR

RESULTS AND DISCUSSIONS

Introduction

This chapter presents results and discussion of the study. It begins with the description of the socio demographic and travel characteristics of respondents. It also analyses tourists' perceived vulnerability of cybercrime and its effect on travel decisions. Again, analyses of tourists' actual cybercrime experiences in Ghana as well as their preventive mechanisms are presented. Finally, the chapter explores the relationship between perceived vulnerability and victimization by respondents' background characteristics.

Socio-Demographic Characteristics of Respondents

The socio-demographic variables covered in the study included; gender, marital status, age, educational qualification, religious affiliation, monthly income and nationality. From the analysis, it was observed that out of the 370 respondents surveyed, females (60.5%) outnumbered their male counterparts (39.5%). This finding is in agreement with the findings of (Boakye, 2012; Mensah & Mensah, 2013). The study was also dominated by respondents who fell between the ages of 21-30 (47.8%), followed by respondents between 31-40 (18.1%), with the least age group being respondents of 61 years and above (4.3%). With country of origin, European tourists dominated the study (n=193 or 52.2%) with America accounting for 35.1 percent and African countries constituting 8.4 percent.

Table 1: Socio-demographic characteristics of respondents (N=370)

Characteristics	Frequency	Percentage%
Sex		
Male	146	39.5
Female	224	60.5
Marital Status		
Single	252	78.1
Married	102	27.6
Divorced	15	4.1
Widowed	1	.3
Age		
Below 20 years	65	17.6
21-30years	177	47.8
31-40years	67	18.1
41-50years	24	6.5
51-60years	21	5.7
61 and above	16	4.3
Nationality		
Africa	31	8.4
Europe	193	52.2
America	130	35.1
Australia	8	2.2
Asia	8	2.2
Level of Education		
Primary school	7	1.9
High school	66	17.8
College/University	211	57
Post Graduate	86	23
Religion		
Christianity	228	61.6
Islam	70	18.9
Atheist	27	7.3
Buddhism	16	4.3
Jewish	11	3.0
Not stated	18	4.9
Monthly income in dollars		
Less than 300	76	20.5
300 to 600	48	13.0
600 to 900	31	8.4
Above 900	135	36.5
Not stated	80	21.6

Source: Fieldwork, (2019)

It is also worth noting that, the least participants of the study in terms of continents of origin were from Australia (2.2%) and Asia (2.2%). The dominance of tourists from European countries is in consonance with the Ministry of Tourism statistics and the findings of Boakye (2012) that, Europe continues to dominate as the major generating region for Ghana with the most mentioned countries being Germany, the United Kingdom and France. This finding also conforms to the report of UNWTO (2011) that, Europe is the world's leading tourist generating region constituting 50.7 percent of the total arrival.

The educational background of respondents also showed that the respondents were generally highly educated since they were basically people who have attained degree (57%) and post graduate (23%). The educational level of the respondents also showed pattern which is similar to those described in the Ministry of Tourism (2015) statistics that, tourists to Ghana are generally highly educated and are mainly engaged in formal occupations. Also, the unmarried respondents (68.1%) outnumbered the married respondents (27.6%). About 4.1 percent of the respondents were divorced whiles 0.3% was widowed.

Concerning tourists respective religious affiliations, more than half (61.6%) of the study sample described themselves as Christians whereas 18.9 percent were Muslims. Meanwhile, 4.9 percent of the respondents didn't make their affiliations known. With respondents' average income, it emerged that 36.5 percent of the respondents earn a monthly income above $900, 22.7 percent did not make their income known.

In all, the study was dominated by females (60.5%) between the ages of 21-30 (47.8%) who came from Europe (52.2%) and were mostly unmarried

(68.1%). This finding could be associated with the fact that Ghana is generally popular among the youth market (Dayour & Adongo, 2015) and also noted to be popular among young tourists particularly from Europe and North America due to its sandy beaches and tropical climate (Dayuour, 2015). Majority of them professed to be Christians (61.6%) with educational background in degree (57%) and most of them earn a monthly income of above $900 (36.5%).

Travel Characteristics of Respondents

This section presents the findings on the travel characteristics of inbound tourists in Ghana. Variables considered include tourists travel experience, the frequency of trip, purpose of visit, as well as their use of electronic cards and Wi-Fi during their stay. The study observed that, greater portion of the respondents were first time visitors (68.9%) with the remaining being repeat visitors (31.1%). The high figure of first timers confirms the finding of Boakye (2012) whose study on inbound tourists was dominated by first time visitors.

Table 2: Travel Characteristics of Respondents (N=370)

Travel characteristics	Frequency	Percentage (%)
Trip Experience		
First time visitors	255	68.9
Repeat visitors	115	31.1
Frequency of trip		
Twice	32	9.2
Three times	38	10.2
3+	43	11.6
Purpose of visitation		
Vacation/Leisure/Holiday	162	43
VFR	72	20.0
Education	51	13.8
Business	28	7.6
Volunteer	55	14.9
Type of accommodation		
Hotel	162	43.8
Guest house	116	31.4
Homestay	92	24.9
Electronic cards and Wi-Fi used		
Wi-Fi;	288	77.8
hotel/airport/restaurant/mall etc.		
Credit card and visa card	170	45.9
ATM card	174	47
None	35	9.5

*the frequencies and percentages of "***electronic cards Wi-Fi used***" exceed the total because it's a multiple response.
Source: Fieldwork, (2019)

Also, it was found that, most of the respondents (43.8%) used hotels during their stay. The most preferred form of accommodation was hotel followed by those who used either guesthouse (31.4%) or homestay (24.9%). It was also revealed that, tourists visited Ghana for diverse reasons or purposes. Out of the 370 respondents, 162 (43%) visited Ghana for the purpose of having a vacation/holiday/leisure. Other purposes of visitation included visiting friends and family (20%), education (13.8%), volunteering (14.9%) and business (7.6%). A little over three quarter (77.8%) of the respondents confirmed to have been using the various public Wi-Fi at the airports, restaurants, malls, banks, and other places they visited. Also, slightly less than half of the respondents (45.9% and 45%) used credit card and Visa card/ATM respectively during their stay.

In summary, the analysis of respondents travel characteristics revealed that, majority of the respondent were first timers (68.9%) whose purpose of visitation was mainly for vacation/leisure/holiday (43%); this finding is in conformity with the pattern of the annual inbound tourists flow into the country as put out by Ghana Tourism Authority (GTA) that, vacation and leisure travelers always dominate amongst the other purposes of visitation. With hotel being the most preferred form of accommodation (43.8%), majority of the respondents also used the Wi-Fi in places such as the airports, hotels, restaurants and malls (77.8%).

Perceptions of Cybercrime Vulnerability in Ghana

As stated by Grabosky and Smith (2001:39), a ‘key principle in the prevention of cybercrime is the need to raise awareness on the part of prospective victims to the risks which they stand to face’. Thus, being aware of a phenomenon pre-informs you on the risks you are likely to encounter. Therefore, respondents were asked to share their views on whether or not they have heard of any cybercrime incident in Ghana. Awareness of risks associated with particular environments or activities is a form of personal guardianship (Ngo & Paternoster, 2011; Sheng et al., 2010), as it allows individuals to take proactive protective measures to avoid victimization. As indicated in figure 3, tourists' awareness about cybercrime incidents in Ghana was generally low.

That is, only slightly above one quarter (26.8%, n=100) of the respondents responded in the affirmative that they have heard about one cybercrime incident or the other in Ghana.

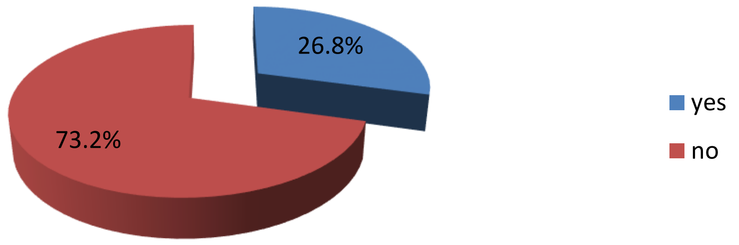

Figure 3: Inbound Tourists Awareness on Cybercrime Victimization in Ghana.

Source: Fieldwork, 2019

The majority of the respondents (73.2%, n=270) indicated that they have not heard of any cybercrime incident about Ghana. This means that a very high percentage of the respondents were not aware of any cybercrime incident as it has been overemphasized by the media. Research findings on cybercrime awareness indicate that on the average, individuals with better awareness of online security are less likely to be vulnerable to cybercrime especially with phishing emails (Halevi, Lewis, & Memon 2013; Sheng et al., 2010). However, Halevi, Lewis, and Memon (2013) again found that a subsection of Internet users despite their level of awareness appear to be highly vulnerable to phishing due to other factors other than lack of awareness.

The respondents who had heard of cybercrime incidents in Ghana were further asked to indicate their source of information on cybercrime incidents in Ghana as well as the forms they have heard of. Regarding the sources through which tourists got their information on cyber victimization in Ghana from, four sources of information were observed; the internet (37.2%), the media (31.4%), family and friends (21.3%) and from the workplace (10.1%).

Also, Table 3 presents the various forms of cybercrime that the respondents had heard of. From the table, fraud and identity theft happened to be the forms with the highest frequencies, with the percentages 58.7 and 17.6 respectively. Other forms were phishing, data manipulations/duplication, blackmail/extortion, and hacking. A deduction could therefore be made from Table 3 that, the major forms of cybercrime in Ghana are fraud, mobile money scams and cyber identity theft. This finding is in agreement with the findings of Barfi, Nyagorme and Yeboah, (2018) which revealed the forms of cybercrime in Ghana to include hacking, credit card fraud, identity theft, and dating fraud.

Table 3: Respondents Perceptions of most Prevalent forms of Cybercrime in Ghana.

Tourist perceptions on the forms of CC	Frequency	Percentage%
Phising/ fraudulent mails	12	8.4
Online identity theft	25	17.6
Fraud; credit card/advance fee/mobile money, sakawa etc.	82	57.8
Manipulations of cash machines	14	9.9
Extortion/blackmail	2	1.4
Hacking	7	4.9

*N=142 Multiple response
Source: Fieldwork, (2019)

Perceived Vulnerability to Cybercrime in Ghana

One key objective of the study was to examine the perceived vulnerability of inbound tourists on cybercrime in Ghana. And so, for clearer understanding of respondents' views on cybercrime vulnerability, the respondents were first asked to share their views on the various ways through which they think internet/phone/computer/technological gadgets and service users are susceptible to cybercrime. The respondents considered the following ways as presented in Table 4, as the various possible ways through which any internet user or digital gadgets user can fall victim to cybercrime. It emerged a little less than quarter (21.8%, n=64) of the respondents claimed it is naiveness or lack of awareness/ignorance on cybercrime that increases one's chance of being prone to cybercrime. This category of the respondents believed that, through ignorance, one can easily be a victim to cybercrime. Other ways of vulnerability provided included but are not limited to sharing or exposing personal and financial information (10.9%), the use of public Wi-Fi (9.6), making friends and partners online (6.1%), among others.

Table 4: Tourists' Views on Ways of Cybercrime Vulnerability

Tourists views on ways of vulnerability	frequency	Percentage%
Making friends and partners online	18	6.1
Not being careful with your internet life	34	11.6
Naiveness/ignorance/lack of awareness	64	21.8
Mobile money and banking	11	3.8
Weak/ no password, pins, codes	26	8.9
Trying to invest or do business online	9	3.1
Sharing of financial information	32	10.9
Use of public Wi-Fi	28	9.6
Online purchases and Bookings	10	3.4
The use of Credit cards and similar	27	9.2

Table 4 Continued

Lack of inadequate internet security	10	3.4
Old systems/ infrequent updates	5	1.7
The use of phones/PCs/internet	19	6.5

*N=293multiple response
Source: Fieldwork. (2019)

Respondents were further asked of the probability of they falling victim to cybercrime. From the findings, a little over a quarter of the respondents (28.6%, n=107) indicated that they felt vulnerable to cybercrime in Ghana with the remaining 71.4 percent not considering themselves to be vulnerable.

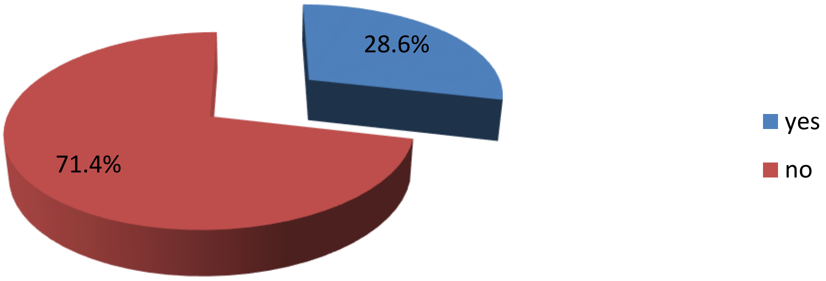

Figure 4: Respondents Perceived Vulnerability to Cybercrime in Ghana

Source: Fieldwork, 2019

To further understand the respondents' perceived vulnerability to cybercrime, the respondents were requested to indicate the reasons for their likelihood of falling victim to cybercrime**.** From the findings, the respondents that claimed to be vulnerable to cybercrime (28.6%, n=107) provided reasons to back their assertion. It came out that, (42%, n=45) of them attributed their vulnerability to their use of the internet, laptop or computers, phones among its related services and applications. These respondents were of the view that, anyone who uses the internet, laptop or computers, phones and its related services and applications are vulnerable in one way or the other to cybercrime.

Hence, they stand a chance of falling victim to cybercrime. Furthermore, other part of the respondents (n=20, 18.5%) shared their views that as tourists, most of them make use of credit cards either online or offline, there is the use of other cards such as ATM and Visa cards which also help facilitate their daily routines. Meanwhile, all these are major tools that cyber criminals take advantage of to defraud people. Other factors provided include the use of unsecured public Wi-Fi, online purchases and bookings.

Considering Felson (1979) Routine Activities Theory in relation to this finding, individuals' involvement in routine online activities that increase exposure to motivated offenders may disproportionately increase the risk of victimization. Also, the theory proposes that there must be some physical visibilities that are likely to affect the target suitability which make the individual vulnerable or attractive to the offender. In the view of Yar (2005), there are numerous targets suitable for predation and these consist of certain online behaviors of respondents which put them at risk of cyber victimization such as putting important personal information or financial information on social media, online payment and purchasing services, or making passwords visible to everyone, as well as computer systems themselves that may be compromised and disrupted by unauthorized intrusion and interference.

To this end, this observation could be related to several studies (Bossler & Holt 2009; Holt & Bossler 2008; Leukfeldt, 2014) who found out that, time spent using e-mail or social media, increases individual risks of interpersonal victimization such as online harassment. In a study by Leukfeldt and Yar (2016) also, online communication, the use of forums or social networks, the use of the internet, targeted and untargeted browsing, online shopping, downloading and gaming were all related to increased hacking and malware virus victimization respectively.

Table 5: Respondents reasons for feeling vulnerable to cybercrime in Ghana

Tourists reasons for perceived vulnerability	Frequency	Percentage%
Am not cautious of my internet life	13	16
I use public Wi-Fi	12	14.8
I use ATM/Credit card etc	15	18.5
I make online purchases and bookings	2	2.5
Because am a first time visitor	4	4.9
Everyone is vulnerable	34	42
Provision of personal details at hotels	1	1.2

**N= 81*multiple response
Source: Fieldwork. (2019)

Notwithstanding, the tourists (n=264, 71.4%) who indicated that they were invulnerable to cybercrime gave interesting reasons for this assertion. As presented in Table 6, out of the perceived invulnerable tourists (n=264, 71.4%), 44.2 percent of them regarded themselves as ‘‘more vigilant to be victimized’’. The second group of respondents also indicated that, as part of preventing themselves from becoming a victim, they avoid the use of smartphones and the internet (34.1%) whenever they are away from home and so, possible ways of making them prone to cybercrime is reduced.

Table 6: Respondents reasons for their perceived invulnerability to cybercrime in Ghana.

Tourist reasons for not being vulnerable to CC	Frequency	Percentage %
I don't use the internet during my stay	44	34.1
I use physical cash in all my payments	15	11.6
I am very vigilant	57	44.2
I don't give out my personal information	1	0.8
I don't book/purchase online	3	2.3
I don't use public Wi-Fi	4	3.1
I have good PC/phone/internet security	5	3.9

**N= 129 M*ultiple response
Source: Fieldwork. (2019)

Respondents' perceptions of other tourists' vulnerabilities to cybercrime in Ghana.

The respondents were again asked to share their views whether or not they see other tourists to be vulnerable to cybercrime. Compared to their personal perceived vulnerability, the story changed when the issue of other tourists' vulnerability was raised. A little above three quarters of the respondents (75.9%, n=296) believed other tourists to be vulnerable to cybercrime. This percentage is almost three times bigger than when the respondents were asked if they see themselves to be vulnerable. This implies that, few respondents see themselves to be vulnerable but the majority sees others to be more vulnerable.

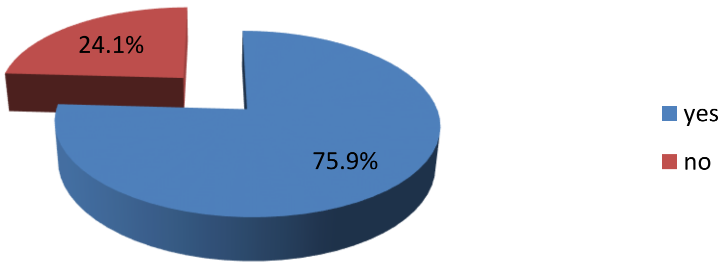

Figure 5: Respondents Perceptions of other Tourists' Vulnerabilities to Cybercrime in Ghana.

Source: Fieldwork, 2019

Interestingly however, most of the respondents (40.6%, n=121) acknowledged other tourists to be more vulnerable to cybercrime mainly because of the 'lack of awareness by most of the tourists'. This finding implies that, tourists perceive others to be not well aware of the tactics and operations of the fraudsters hence their likelihood of falling victims. Again, because these tourists are also into the use of gadgets (28.2%) like (phones, laptop and its services such as email, SMS, social media, among others), chances are that, they may fall prey into the hands of online scammers. Other factors included the use of credit cards (14.7%), online bookings (2.9%) among others as presented in table 7. These findings suggest another dimension to Stanko's (2000) 'paradox of fear' the fallacious perception of lower vulnerability. In such a fallacy, people consider themselves to be less vulnerable than others while in reality, they are at a higher a risk. This is also supported by the findings on perceived vulnerability and victimization. From the findings, respondents that claimed to be invulnerable to cybercrime and yet got victimized (n=21, 54%) were more than those who even professed to be vulnerable (46%, n=18).

Table 7: Factors accounting for other tourists' Vulnerability to Cybercrime in Ghana

Factors for other tourists vulnerability	Frequency	Percentage %
Online purchases/shopping	2	1.2
The use of phone and related services; emails, etc	17	10.0
The use of credit cards/ATM/Visa card etc	25	14.7
Booking	5	2.9
Naiveness/ lack of knowledge on Cybercrime	69	40.6
Scammers are smart	4	2.4
Everyone who uses the internet/PC is vulnerable	48	28.2

*N=170 Multiple responses
Source: Fieldwork. (2019)

Perceived vulnerability to cybercrime is noted to have associations with socio-demographic characteristics such as age (Button et al., 2014; Schoepfer & Piquero, 2009). On this basis, the perceived vulnerability of respondents on cybercrime in Ghana was subjected to further analysis to determine which of the socio-demographic variables felt vulnerable the most using the chi square test of independence. The result of this analysis is presented in Table 8.

Table 8: Tourists' background characteristics by perceived vulnerability

Socio demographics	N	Yes	No	X(df)	P-Value (P>0.05)
Gender					
Male	146	43(29.45)	103(70.55)	0.0762(df=1)	0.783
Female	224	63(28.13)	161(71.88)		
Age					
Below 20 years	65	17(26.15)	48(73.85)	10.562(df=5)	0.061
21-30years	177	42(23.73)	135(76.27)		
31-40years	67	29(43.28)	38(56.27)		
41-50years	24	8(33.33)	16(66.67)		
51-60years	21	7(33.33)	14(66.67)		
61+	16	1(18.75)	13(81.25)		

Table 8 Continued

Level of education					
Primary	7	1(14.3)	6(85.71)	12.952(df=3)	0.005
High school	66	22(33.3)	44(66.67)		
University/college	211	47(22.3)	164(77.73)		
Post graduate	86	36(41.9)	50(58.14)		
Marital status					
Single	252	66(26.19)	186(73.81)	3.379(df=3)	0.337
Married	102	36(35.29)	66(64.71)		
Divorced	15	4(26.67)	11(73.33)		
Widowed	1	0(0.00)	1(100.0)		
Continents of origin					
Africa	31	6(19.35)	25(80.65)	3.0493(d=3)	0.550
Europe	193	52(26.94)	141(73.06)		
America	130	42(32.31)	88(67.69)		
Australia	8	3(37.50)	5(62.50)		
Asia	8	3(37.50)	5(62.50)		
Monthly income ($)					
Less than 300	76	18(23.68)	58(76.32)	2.505(d=4)	0.644
300-600	48	12(25.0)	36(75.0)		
600-900	31	10(32.26)	21(67.74)		
Above 900	135	44(32.59)	91(67.41)		

Source: Fieldwork. (2019)

Female tourists who felt vulnerable to cybercrime in Ghana were about 28.13 percent while relatively same proportion (29.45%) of male tourists felt vulnerable. The chi square test result, however, revealed that no significant relationship (p=0.0762) existed between the variable sex (male and female) and the perceived vulnerability of respondents.

In terms of respondents' age and perceived vulnerability, the findings did not record any statistical association with a p-value of (p=0.061). Majority of the respondents who did not feel vulnerable (81.25%) were respondents of 60years and above. Tourists who were within (31-40) years had the highest percentage of vulnerability (43.28%) while those in 61years and above had the lowest; this finding is quite similar to the study of Norton Cyber Security (2016) that those who are born between 1982 and 2004 are among the top victims of cybercrime. This could mean that, the youthful age that are more active and curious fall under the computer centric generation are more exposed to the world through certain ICT applications and network.

It was noted that there was a significant association between respondents' education and their perceived vulnerability to cybercrime with a p-value of (p=0.005). From Table 8, 41.86 percent of respondents with post graduate education had the highest percentage of vulnerability which happened to be the majority. About 33.33 percent of respondents with high school education claimed to be vulnerable to cybercrime whereas (22.27%) and (14.29%) of perceivedly vulnerable respondents were observed in respondents with university education and primary education respectively. Therefore, respondents with post graduate education had the highest level of vulnerability while those with primary education had the lowest. This is probably because more educated individuals tend to spend more time online and to make online purchases (Pratt et al., 2010) and possibly, internet users that are more educated have higher computer self-efficacy, which could lead to carelessness (Wright & Marett, 2010).This finding also contrast with Alshalan, (2006) and Van Wilsem, (2011) who found no direct association between education and general fear of cybercrime.

Again, no significant relationship was recorded (*p-value* = 0.337) between respondents' marital status and their perceived vulnerability to cybercrime. This is because, whereas the married group recorded the highest percentage of vulnerability (35.29%), respondents with single status and divorced status recorded almost the same percentage of perceived vulnerability (26.67% and 26.19%) respectively. The only one respondent with widowed status had no perceived vulnerability of cybercrime. Therefore, respondents with the highest percentage of vulnerability are the married respondents whereas the divorced group the lowest.

The Chi square test of independence again showed no significant relationship between respondent income and their perceived vulnerability to cybercrime with a p-value of (p=0.644). Majority of the respondents who felt vulnerable were those within the income range of $600-$900 and those who receive above 900 dollars with percentages of (32.26 and 32.59) respectively. Between the income range of 300 and 600 dollars, (25%) of the respondents felt vulnerable to cybercrime whereas 23.68 percent of respondents who receive less than 300 dollars felt vulnerable. Additionally, majority of tourists with income less than 300 dollars who felt invulnerable (76.32%) were almost the same as tourists with (300-600) dollars (75%) who said they were not vulnerable to cybercrime. This finding is in consonance with the findings of Alshalan, (2006) who found no direct association between income and vulnerability of cybercrime.

The results therefore suggest that, the perceived vulnerability of inbound tourists on cybercrime in Ghana is not related to respondents' sex, age, income, marital status and continents of origin or income but rather, respondents' level of education. Traditional crimes unlike cybercrime establish link between certain demographic characteristics such as income and social status with one's vulnerability to crime (Collins & Emily, 2018; Kanan & Pruitt, 2002), but the case differs as far as the issue of cybercrime is concerned since they occur in different context.

Then again, some selected travel characteristics of respondents were also analyzed with a chi-square test by respondents' perceived vulnerability to cybercrime in Ghana. Throughout the analysis of respondents travel characteristics against perceived vulnerability to cybercrime, the chi-square test of independence recorded no significant relationships between respondents travel characteristics and their perceived vulnerability of cybercrime as presented in Table 9.

Although the variables did not return a significant score, there were notable differences across the various categories. Regarding trip experience, first time visitors who declared to be vulnerable to cybercrime constituted about seventy percent (70.8%) compared to the small size (29.2%) of the repeat visitors. This finding relates to the finding of George (2010) who found first time tourists to be more susceptible to crime and feel less safe than those who have ever visited the destination. For the frequency of visit, respondents of two-time visitation recorded 32.3 percent vulnerability, with tree times and more than three times recording 35.48 and 32.25 percentages respectively.

Table 9: Tourists' Travel Characteristics by Perceived Cybercrime Vulnerability

Travel characteristics	N	Yes(%)	No(%)	X (df)	P-Value
Trip experience					
First time visitors	255	75(29.41)	180(70.59)	0.234(df=1)	0.629
Repeat visitors	115	31(26.96)	84(73.04)		
Frequency of trip					
Twice	34	10(29.41)	24(70.59)	0.4797(df=2)	0.787
Three times	38	11(28.95)	27(71.05)		
3+	43	10(23.26)	33(76.74)		
Purpose of visit					
Leisure/Vacation/Holiday	162	51(31.48)	111(68.52)	3.362(df=4)	0.499
VFR	74	16(21.62)	58(78.38)		
Education	51	13(25.49)	38(74.51)		
Business	28	10(35.71)	18(64.29)		
Volunteer	55	16(29.09)	39(70.91)		
Accommodation type					
Hotel	162	52(32.10)	110(67.90)	1.679(df=2)	0.432
Guesthouse	116	30(25.86)	86(74.14)		
Homestay	92	24(26.09)	68(73.91)		

Source: Fieldwork, (2019)

In all the categories of the purpose of visitation, vacation travelers happened to have had the highest percentage of vulnerability (48.11%) compared to 15.09 percent of travelers visiting friends and family, 15.09 percent of volunteer tourists, 12.26 percent of educational tourists and 9.43 percent of business travelers. With respect to respondents' accommodation choice, hotel users perceived themselves to be more vulnerable compared to any other accommodation facility users. Thus, while almost half of hotel users (49.06%) claimed to be vulnerable, only slightly more than one quarter (28.3%) of guesthouse users and slightly less than one quarter of respondents who used homestay (22.64%) perceived themselves to be vulnerable.

The Effect of Perceived Vulnerability on Travel Decisions

This section explores how respondents' perceived vulnerability shapes their routine online behavior at the destination. Therefore, respondents were first asked if they do consider the issue of cybercrime when planning for their trips or before choosing a particular destination over the other. With this, about (69.7) percent of the respondents expressed that they do not while the remaining (30.3%, n=111) responded positive to it. This suggests that, the influence of perceived vulnerability of cybercrime on travel decisions is not a major consideration since slightly more than a quarter of the respondents include cyber issues in their travel decisions compared to those who do not. From the few that include cybercrime in their decisions, they were further asked if they have ever rejected a destination based on its cybercrime issues. About 89.7 percent of the respondents said they have not rejected any destination based on its cybercrime issues. Only 10.3 percent professed of rejecting or choosing one destination over the other due to the nature of the destination's cybercrime issues.

Since another key objective of the study was to determine how the perceived vulnerability influence tourists travel decisions, respondents were asked to express their adoption and use of electronical devices, its networks and applications because these are the ultimate means through which people could become vulnerable and victimized. Although electronic devices can be extremely useful to international travelers, particularly for recording their travels and communicating with family and friends through speaking into a cell phone or creating text messages. Meanwhile, the use of these electronical gadgets and appliances influences ones likelihood of becoming victim to cybercrime. It could be observed from figure 6 that, about 91.3 percent of the respondents travelled with their smartphones in order to be able undertake certain task/functions such as, make bookings, making orders, communicating with service providers and family among others. Other devices travelled with include laptops, ipad/kindles, and hard drives/pen drives. It was also observed that, some small portion (2.7%) of the respondents preferred travelling with durable, cheap phone that can be used in public without worrying about someone stealing it or using the internet.

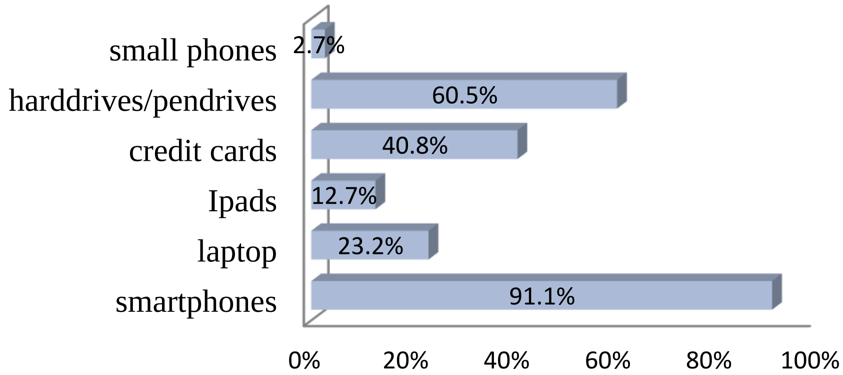

Figure 6: Electronic Devices Respondents Travelled with

Source: Fieldwork, 2019

Also, the RAT theory posits that, certain routine online behaviors and activities put people at risk of cyber victimization. Based on the theory and respondents perceived vulnerability, respondents were asked to express whether or not they use the internet and its related services which could increase their level of victimization. From the study, it was observed that not all the respondents use the internet/smartphone during their stay. About 91.9 percent of the respondents indicated that they use the internet. The findings of Dayour, Park and Kimbu (2019) revealed that, an insightful way of dealing with the physical risk of losing a smartphone in Ghana was to use a cheaper cellphone at the destination. In their study, some respondents stated that it would be more disturbing for them to lose an expensive mobile phone in comparison to a cheaper one. And moreover, holding an expensive one will predispose them to criminal attacks. This implies that, it is sometimes preferable for some tourists to leave expensive communication gadgets at home while traveling outside their country since they have the ultimate responsibility and accountability for their security and privacy in most countries.

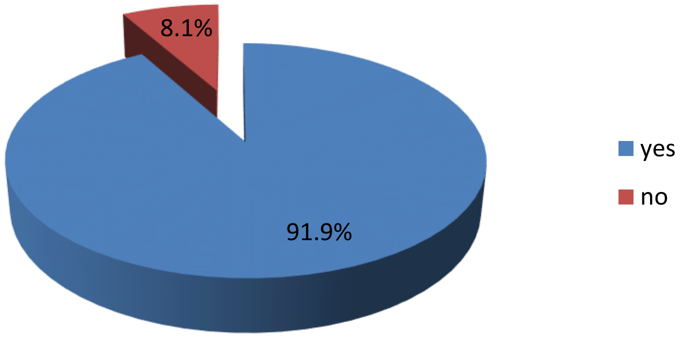

Figure 7: Respondents use of Internet/Smartphone while in Ghana

Source: Fieldwork, 2019

Concerning the use of the internet, 36.2 percent of the respondents use the internet for social media (Facebook, Instagram, Twitter, WhatsApp, among others) to get in touch with friends and family at home, upload pictures and videos of their experiences among others while in Ghana. This finding is in line with that of Dayour et al., (2019), who found the topmost activity undertaken by tourists with their smartphones to be social media networking, such as Facebook, WhatsApp, Instagram, and Snapchat among others. Notwithstanding, other uses mentioned include information search on accommodations, attractions, the use of GPS among others, the news, shopping, booking, sports/YouTube, and others as presented in Table 11. All these practices and routine behavior increases respondents' chances of victimization in the absence of capable online guardianship.

Table 10: **Respondents Routine Online Activities**

Respondents Routine Online Activities	Frequency	%
Leisure/TV/Music/YouTube/sports/	65	13
Information search; Google map, study, etc.	117	23.4
News	34	6.8
Shopping	8	1.6
Social media	181	36.2
Blogging	7	1.4
Booking	35	7
Work	38	7.6
Mobile money/banking	4	0.8
Uber	11	2.2

* *N=500* Multiple response
Source: Fieldwork. (2019)

Tourists' Experiences of Cybercrime in Ghana

Pertaining to the specific objectives of the study, respondents' experiences of cybercrime in Ghana were also explored. As a result, respondents were first asked whether or not they have fell victim to any form of cybercrime in Ghana. It emerged from the study that the actual cybercrime experiences of inbound tourists was quite low. That is, only 10.5 percent (n=39) of the respondents have been a victim to cybercrime either during their stay in Ghana or while in their home country but got victimized by a Ghanaian through the internet and mostly through the social media. The remaining respondents (89.5%) affirmed not to have experienced any form of cybercrime in Ghana or by any Ghanaian.

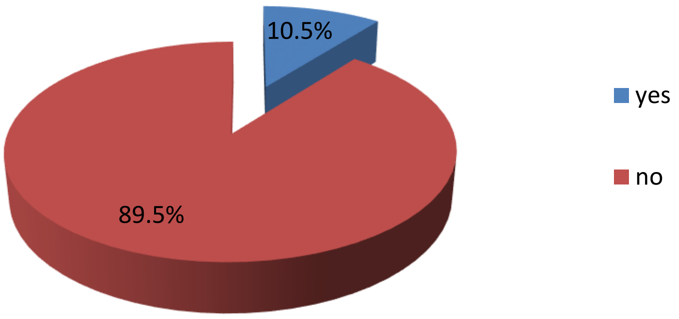

Figure 8: Respondents Experiences on Cybercrime Victimization.

Source: Fieldwork, 2019

The reason for this small percentage of victimization could be in accordance with the assertion of the Criminal Investigation Department (CID) that, victims of cybercrime are usually a high-profile individuals or rich expatriates who cannot face the embarrassment of people knowing that they have been duped or as reported by Ghana Tourism Authority (GTA) that Ghana's inbound visitors are generally known to be young low income millennials. As asserted by Scheibler, Crotts and Hollinger (1996) and Allen, (1999) also; crimes against tourists are relatively low meanwhile it is the media that has overemphasized the incidents or ham it up to make the entire destination appear insecure or unprotected.

Individuals' background characteristics are also noted to have relations with victimization (Boakye, 2012; Trahan et al., 2005; Ganzini et al., 1990). In this regard, relationship between victimization and socio-demographic characteristics using the chi square test of independence was explored. The result of this analysis is presented in table 11.

Table 11: Respondents Socio-Demographic Characteristics by Victimization

Socio-demographics	N	Yes f(%)	No f(%)	X(df)	P-Value (P=0.05)
Gender					
Male	146	20(13.70)	126(86.30)	2.551(df=1)	0.110
Female	224	19(8.48)	205(91.52)		
Age					
Below 20years	65	5(7.69)	60(92.31)	8.222(df=5)	0.144
21-30	177	16(9.04)	161(90.96)		
31-40	67	13(19.40)	54(80.60)		
41-50	24	1(4.17)	23(95.83)		
51-60	21	3(14.29)	18(85.71)		
60+	16	1(6.25)	15(93.75)		
Level of education					
Primary	7	1(14.29)	6(85.71)	1.028(df=3)	0.795
High school	66	9(13.64)	57(86.36)		
University/College	211	20(9.48)	191(90.52)		
Post graduate	86	9(10.47)	77(89.53)		
Marital status					
Single	252	24(9.52)	228(90.48)	1.730(df=3)	0.630
Married	102	14(13.73)	88(86.27)		
Divorced	15	1(6.67)	14(93.33)		
Widowed	1	0(0.00)	1(100.0)		
Continents of origin					
Africa	31	5(16.13)	26(83.87)	3.175(df=4)	0.529
Europe	193	18(9.33)	175(90.67)		
America	130	13(10.00)	117(90.0)		
Australia	8	2(25.00)	6(75.0)		
Asia	8	1(12.50)	7(89.46)		
Monthly income ($)					
Less than 300	76	6(7.89)	70(92.11)	2.685(df=4)	0.612
300-600	48	7(14.58)	41(85.42)		
600-900	31	3(9.68)	28(90.32)		
900+	135	12(8.89)	123(91.11)		
Not stated	80	11(13.75)	69(86.25)		

Source: Fieldwork, (2019)

Male respondents who got victimized (13.70%) outnumbered their female counterparts (8.48%). The chi square test recorded no significant relationship between gender and cybercrime victimization (p=0.1440). Male victimized respondents exceeding females endorses the findings of (Henson, Reyns &Fisher, 2013; Pereira, Spitzberg & Matos, 2016) which revealed that, women are more concerned than men especially when it comes to cybercrime that involves interpersonal contact such as cyber harassment.

It was again noted that there was no significant association with respondents age and victimization (p=0.144). This is because, almost the same level of percentage of victimization was observed across all the age categories. Respondents within the age range (31-40) years got victimized the most (19.40%). Even within the age range of lower frequencies (51-60 and 60+), there were some form of victimization (14.29% and 6.25%) respectively. This implies that, age do not have any influence on cybercrime victimization.

No significant relationship was again observed between respondents level of education and cybercrime victimization with a p-value of (p=0.795). Respondents from all the educational levels suffered almost the same percentage of victimization (either a little below ten percent or little above ten percent). Thus, whereas 14.29 percent of respondents with primary education got victimized, a little above 10 percent (10.47%) of post graduates got victimized which is almost the same as degree holders (9.48%) who got victimized.

The marital status of respondents equally did not have any significant relationship with victimization (p=0.630). From the different marital statuses, there were some percentages of respondents who have experienced victimization except the widowed. Married respondents recorded higher level of victimization whereas the widowed recorded no victimization (0.00%).

The continents of origin show that respondents from Australia were victimized most (25%) compared to Africa (16.13%), Asia (12.5%) and the Europeans recorded the least percentage of victimization (9.33%). With this result, no significant relationship was again observed (p=0.529). It could therefore be concluded that, respondents' victimization or experiences of cybercrime in Ghana is not influenced by any of their socio demographic variables (age, gender, level of education, marital status, continents of origin and income).

Table 12 presents the victimization of inbound tourists on cybercrime in relation to their travel characteristics such as their trip experiences, frequency of their visit, purpose of visit and the services used during their stay in Ghana. Tourists' victimization of cybercrime was first examined with whether respondents are first time or repeat visitors. With a p-value of (p=0.00), the result indicated a significant relationship which showed that, the trip experiences of respondents have influence on their experiences of cybercrime. That is, first time tourists who got victimized of cybercrime accounted for only 6.27 percent while Repeat visitors who encountered victimization were observed to be 20 percent.

Table 12: Respondents Travel Characteristics by Victimization

Travel characteristics	N	Yes, f(%)	No, f(%)	X^2 (df)	P-value (P>0.05)
Trip experience					
First time visitors	255	16(6.27)	239(93.73)	15.835(df=1)	0.00
Repeat visitors	115	23(20.0)	92(80.00)		
Frequency of visit					
Twice	34	8(23.53)	26(76.47)	1.5696(df=2)	0.456
Three times	38	9(23.68)	29(76.32)		
3+	43	6(13.95)	37(86.05)		
Purpose of visit					
Leisure/vacation	162	30(18.52)	132(81.48)	21.302(df=4)	0.000
VFR	74	2(2.70)	72(97.30)		

Table 12 continued

Education	51	1(1.96)	50(98.04)		
Business	28	1(3.57)	27(96.43)		
Volunteer	55	5(9.09)	50(90.91)		
Accommodation type					
Hotel	162	11(6.790	151(93.21)	4.695(df=2)	0.096
Guesthouse	116	17(14.66)	99(85.34)		
Homestay	92	11(11.96)	81(88.04)		

Source: Fieldwork, (2019)

Tourists' purpose of visitation was observed to have some level of influence on cybercrime victimization since there existed a significant relationship (p=0.00) between the two variables. In terms of respondents who have experienced cybercrime, leisure/vacation tourists were the most victimized while educational tourists recorded the least. Table 12 depicts that, 18.50 percent of the respondents that visited for leisure/holiday/vacation had experience cybercrime. About 9.09 percent of volunteer tourists have been victimized followed by business travelers/tourists (3.57) and then respondents who visited for VFR (2.7%). The least victimized group in terms of purpose of visit accounted to 1.96 percent of the victimized respondents (educational tourists).

Respondents who declared to have repeated their visit to the country were made to report the number of times they have visited Ghana. Repeat visit was operationalized on three categories (twice, three times and more than three times). About 23.53 percent of the respondents with two times visitation experienced victimization which is relatively the same as the respondents with three times visitation (23.68%) followed by the least victimized group (13.95%) of those who have visited the country more than three times. The result of the analysis did not indicate any significant relationship (p=0.456) between respondents' frequency of visit and victimization of cybercrime.

Again, no significant relationship (0.096) was found between respondents' choice of accommodation and their experiences of cybercrime. The highest victimization was observed on respondents who used guesthouses (14.66%). About 11.96 percent of homestay visitors suffered cybercrime victimization. The least group of victimization was those that used hotels (6.79%).

The Nature of Cybercrime Experiences

Regarding the victimized tourists (n=39, 10.5%), the findings revealed that, 59 percent of them have suffered or experienced fraud, more specifically credit card, advanced fee fraud, business fraud, romance fraud and uber fraud. This was followed by phishing (fraudulent mails) (15.4%, n=6) and identity theft/hacking (15.4%, n=6) with extortion/blackmail being the form with the least frequency as presented in figure 9.

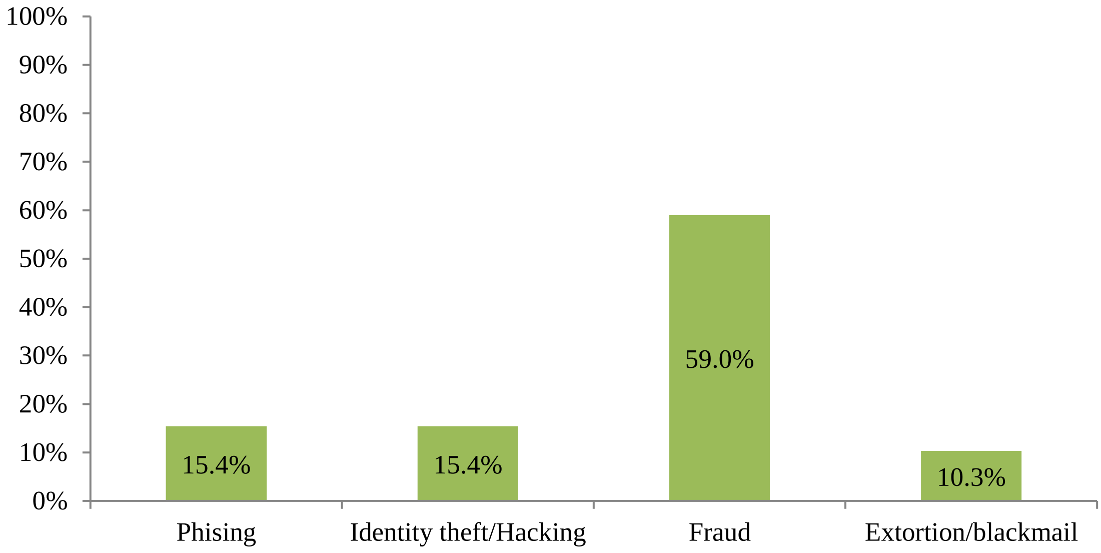

Figure 9: Forms of Cybercrime Experienced in Ghana

Source: Fieldwork, 2019

A deduction can therefore be made that, the most prevalent form of cybercrime that respondents experienced were fraud (credit card fraud, romance fraud/sweetheart swindle, advance fee fraud and business or investment fraud), phishing, identity theft/hacking and extortion. This finding is similar to the findings of Warner (2011), who identified three main forms of cybercrimes prevailing in Ghana to be identity fraud, fake gold dealers and estate fraud. However, Warner conceded that the list is not exhaustive given the fact that technology keeps evolving by the day. Also, the finding is in agreement of the findings of Chawki (2009), which revealed that Advance fee fraud is one of the major scam schemes being carried out in Nigeria. Moreover, cases of online fraud pertaining to credit card crimes, contractual crimes, offering jobs, and advanced fee fraud have been fairly documented in literature (Magele, 2005; Longe et al., 2009).

It was imperative however to determine the number of times respondents might have suffered from cybercrime (CC) victimization. From the finding in Figure 9, first time victims dominated with the percentage of 61.5. The study also recorded second time victims (23.1%), third time victims (7.7%) and even those who have had more than three times experience. Aside the respondents with "ones" experiences, the multiple experiences could not capture whether or not it is the same crime or different kinds of CC that they experienced.

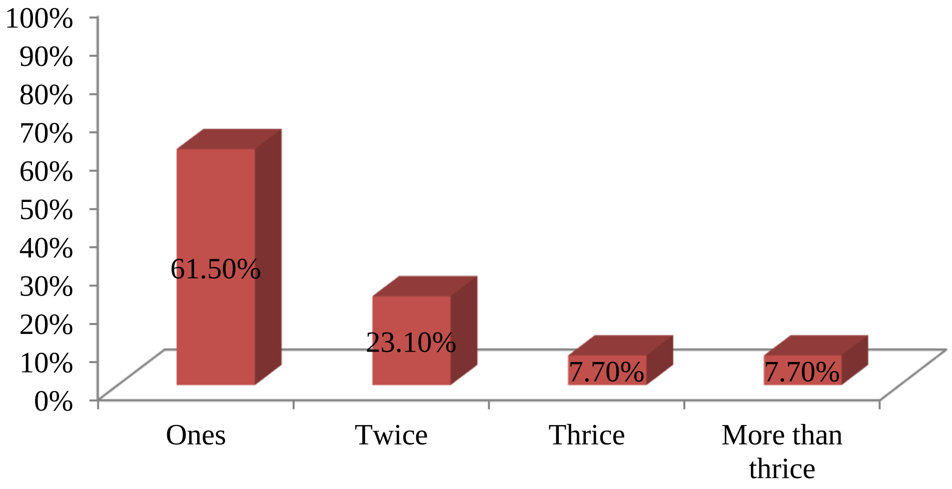

Figure 10: Frequency of Cybercrime Experiences in Ghana

Source: Fieldwork, 2019

It was also revealed from the findings that not all the victimized tourists lost money to their perpetrators. Respondents were asked to indicate whether or not they lost money to cybercrime offenders. The result proved that, the majority of the respondents (64.1%, n=25) lost money to Ghanaian cyber criminals either through being lured into fake businesses, fake relationships, or through the use of stolen financial details. The remaining 35.9 percent might have played smart for not forwarding monies to cyber criminals or being careful with their codes and accounts.

Post Victimization Behaviour on Ghana

The post victimization behaviour of the respondents was operationalized as; the steps respondents took after they got victimized, whether or not they reported the case, kept it to themselves or blocked the source from which they got scammed or victimized.

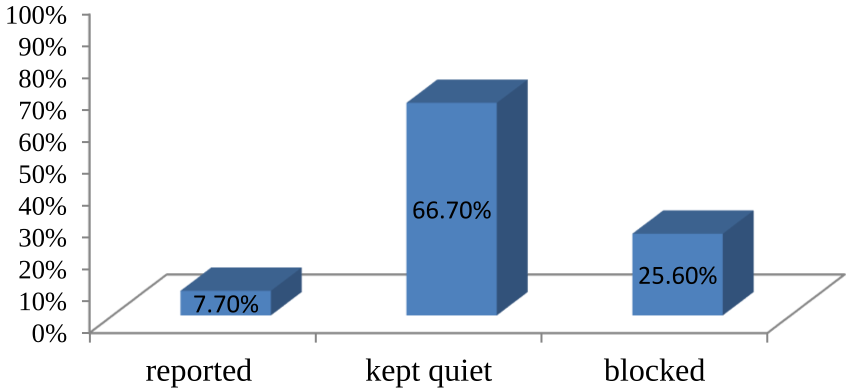

Figure 11: Post Victimization Behaviour of Respondents.

Source: Fieldwork, 2019

As indicated in Figure 11, out of the 39 victimized respondents, only 3 of them (7.7%) claimed to have reported the case to appropriate authorities. For further understanding, the victimized respondents that reported their victimization were requested to share on how they went about it. One of the respondents refused to go further with it but the remaining two who both happened to have suffered from the same crime revealed they reported after their realization of being overly charged on their credit cards after which the stolen monies were refunded to them.

According to Lynch (2014), only a small percentage of cyber-crimes are reported to the police or appropriate authorities, for instance, an estimated 120 to 150 reports per 1,000,000 cybercrimes in the United Kingdom. This finding is in line with the current study in which the majority (26, 66.7%) of the victimized respondents did not report the case but rather kept it to themselves. Ennin (2015) finding also revealed that, foreign victims who wanted to pursue the case of cybercrime victimization were advised by their Ambassadors to pull out for lack of confidence in the Ghanaian legal system, which has been tainted with corruption and undue delay of cases. These factors might have accounted for the low reporting rate on victimization.

Aside this fact, the virtual space unlike the offline or traditional forms of crime is characterized by high level of anonymity and so, it is sometimes difficult on the side of the victim to be able to identify the offender. Again, reluctance to report cybercrimes may also be due to embarrassment, lack of knowledge on where or how to report the crime, or the small size of the loss (Lynch, 2014). Some, especially identity theft victims, may not realize their victim status until sometime after the criminal act when they are denied a loan or other services because of a poor credit rating. The remaining 10 respondents (25.6%) also blocked and deleted the various sources of these scams either through emails, social media, calls, SMS or others.

It was again imperative to probe further in relation to victimized respondents pre-victimization and post victimization perceptions on Ghana as destination. As a result, victimized tourists were asked if their being a victim has in any way changed or influenced their perception on Ghana as a safe tourist destination. About 76.9 percent of the victimized tourists revealed that, their perceptions about Ghana remain the same and they said this on the basis that cybercrime issues are everywhere (75%) and also there are other more positive experiences they have had which surpasses their experiences on cybercrime as presented in Figure 12.

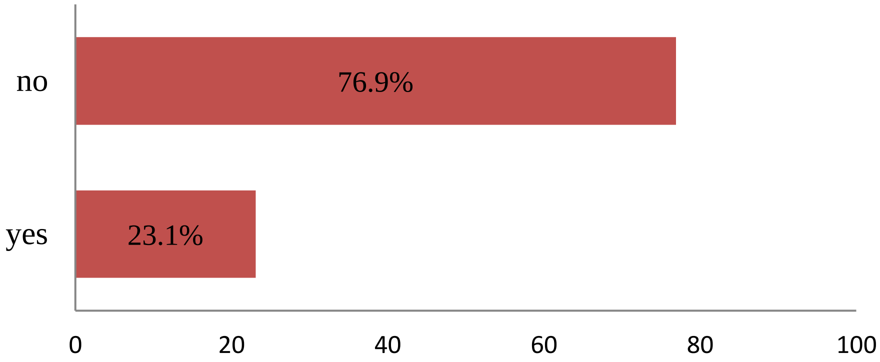

Figure 12: Impacts of Victimization on Tourists' Perception of Ghana.

Source: Fieldwork, 2019

Regarding the victimized tourists', 92.3 percent (n=36) agreed to repeat their visit. This implies that, the desire to revisit the country was strong even among respondents who had fallen victims to one cybercrime or the other during their stay in Ghana. This finding is in line with the finding of George (2003) who observed that in spite of the high rate of crime in Cape Town, 50 percent of the respondents indicated their desire to return. Similarly, Mawby (2000) also reported that 56 percent of tourists who fell victim to crime were positive of returning to the destination. The dominance of the willingness to repeat visit suggests positive perceptions which suggests that being a victim of crime does not necessarily negatively affect repeat patronage. On the contrary, Allen (1999), Brunt and Sheperd, (2004) and Tarlow (2009), suggest that being a victim of crime at a destination negatively influences the potential of repeat visits.

Generally, the majority of the total respondents (93.4%, n=309) also revealed that they will repeat their visit to Ghana. The basis of this assertion are that, about (30.7%) of the respondents claim to like Ghana and for that matter will visit again and (17.6%) of the respondents think there are beautiful attractions to be visited. Other reasons provided include; tourists feeling safe during their stay, tourists enjoying their visit and having wonderful experiences, the need for cautiousness, tourists having a family here and tourists lose being refunded. Notwithstanding, the remaining 6.8 percent of the respondents emphatically made it clear that, they may not repeat their visit to Ghana because as tourists they look out for new discoveries and experiences and for that matter, they would rather want to explore other countries they have not been to rather than visiting where they have been before.

With regards to tourists post visit intention in relation to their willingness to recommend Ghana to others, 89.7 percent of the victimized tourists professed their willingness to recommend. In the whole, 93.4 percent of the total respondents said that they are more than willing to express their positive experiences to others. These respondents supported their aforementioned claim that, compared to other countries visited, Ghana is more safe (23.5%), others also expressed or attributed their reason or willingness to recommend on the fact that Ghana is peaceful and most of its citizens are friendly (23.5%), some also said that that since they have not had any problem or any negative experiences, nothing stops them from sharing the positives. About 2.7 percent of the respondents also expressed that, although they will recommend, but they will tell them to be vigilant since scammers are smart and are everywhere.

Aside respondents’ personal experiences on cybercrime, further analysis was made on respondents’ views on the victimization of other tourists which they might have heard of or witnessed. From Figure 13 it was revealed that, 13.5 percent of the respondents confirmed knowing some tourist(s) who have suffered one form of cybercrime or the other with the remaining 86.5 percent of the population responding negative.

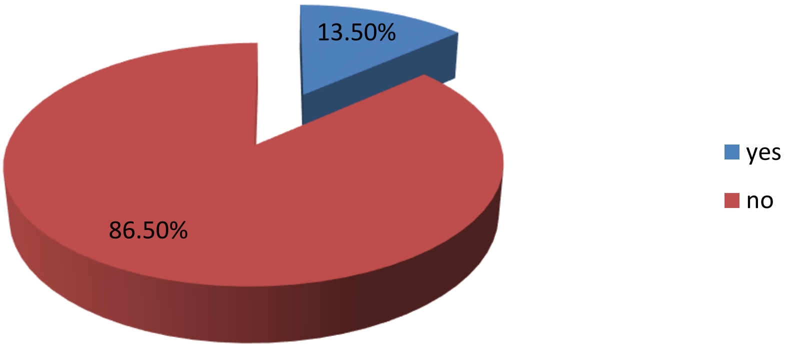

Figure 13: Respondents' Awareness about other Tourists' Victimization.
Source: Fieldwork, 2019.

The various types of cybercrime suffered were therefore made known. Surprisingly, the types experienced were almost the same as those that were experienced by individual tourists themselves. Again, fraud remained the most experienced form of cybercrime with the percentage of 52. Thus, out of the 50 respondents, 26 of them have heard or seen tourists who have fallen victims to fraud. Other forms were phishing, identity theft, dating scams, advance fee fraud, and extortion/blackmail which happened to be the form with the least frequency of 1(2%).

Deployed Strategies to Cybercrime Prevention

Guardianship is measured based on specific online variables employed by the respondents. With online guardianship or coping strategies being another key objective of the study, respondents were asked to share the various ways through which they protect themselves from being victimized. The basic assumption was that, the fact that one is not a victim today does not guarantee his or her safety tomorrow. In this sense, it was imperative to identify the views of respondents on this aspect of cybercrime issue.

Reyns, Henson and Fisher (2011), argued that the mere presence of one of these preventive elements would deter potential offender from perpetrating the crime. The presence of measures like firewalls, security programs, complex codes and pins, and effective law mechanism among many others can help prevent intruders from having access into peoples' accounts and privacy (Reyns et al., 2011).

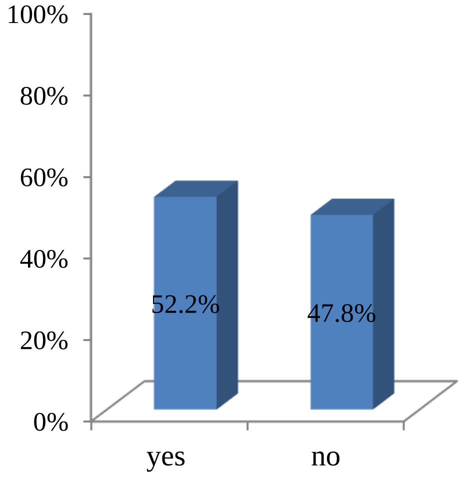

Figure 14: Respondents Awareness of of Preventive mechanisms
Source: Fieldwork, 2019

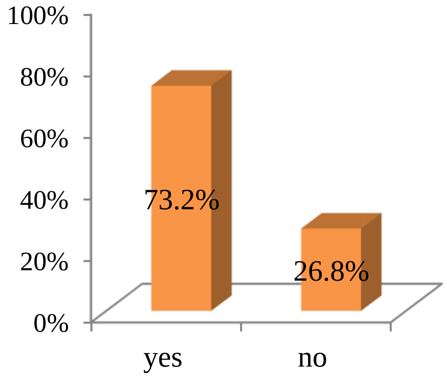

Figure 15: Respondents Adoption CC Preventive CC mechanisms.
Source: Fieldwork, 2019

From Figure 14, it is observed that, 52.2 percent of the respondents think there are ways through which one can prevent him or herself from falling victim to cybercrime but the remaining 47.8 percent had a different view that, there are no preventive strategies to cybercrime. This implies that, as some respondents think there are ways of cybercrime prevention, some also think nothing can be done to prevent cybercrime from occurring. Talking of the implementation of these strategies, Figure 15 proves it that, 73.2 percent of the population indicated a "yes" as an answer. This implies that, the remaining 26.8 percent do not used any form of preventive strategies. It could also be that, although they practice some of these strategies but they have no idea that they (these strategies) are part of the strategies that can help them in one way or the other from cybercriminals.

Table 13: Respondents Suggested Preventive Measures to Cybercrime

Deployed strategies to cybercrime	Frequency	%
Safe websites	50	13.5
Avoid/limit the use of ATM and the likes	36	9.7
The use of only trusted Wi-Fi/turn off Bluetooth when not in use	31	8.4
Avoid making friends and partners online	11	3.0
Not sending money to unknown people	12	3.2
Don't share personal/financial information with anyone	40	10.8
Not opening junk mails and SMS	24	6.5
Careful online esp. social media	31	8.4
Strong antivirus	30	8.1
The use of VPN	13	3.5
Strong/complex password; pin, codes, pattern etc	49	13.2
RFID	2	0.5
Don't bring gadgets at all	5	1.4
Avoid picking unknown numbers	6	1.6

* N=340 Multiple response
Source: Fieldwork. (2019)

It is observed from Table 13 that, respondents stated a number of strategies or tools they use to prevent themselves from victimization. It could also be seen that, the strategies with the leading percentages are; the use of safe and secured websites (13.5%) and the use of strong/complex password (pin, codes, pattern, among others). Other deployed strategies included, not sharing personal/financial information with anyone (10.8) and avoiding/limiting the use of cards (9.7%); especially the use of credit cards online and in all your transactions. Most of the tourists said that, they prefer using physical cash in all their transactions than the card and their major reason for doing this is to be safe from fraudsters stealing their details or tracing their card codes especially on the internet.

This finding is similar to that of Dashora (2011) that, every internet user should avoid; disclosing any information pertaining to one self, sending credit card number to any site that is not secured and rather use latest and update antivirus software to guard against virus attacks. Also, it is similar to the strategies proposed by Norton (2018) that, the use of a full-service internet security suite, the use of strong and complex passwords and frequent update of software can help prevent cyber victimization. This finding is again similar to the findings of Zhang and Prichard (2009) whose survey observed the internet users security practices to include software updates, firewall usage and the anti-virus/anti-adware/anti-spyware practices.

As the Routine Activities Theory proposes, crime occurs during every-day routines in normal life when a suitable target is in the presence of a motivated offender who is without a capable guardian; online preventive mechanisms to cybercrime (Cohen & Felson 1979). The basic assumption is that, there exist an inverse relationship between capable guardianship and victimization. Meanwhile, the Chi-square test revealed an unexpected outcome between guardianship and victimization. There existed a significant relationship (p=0.024) between victimized respondents and their implementation of cybercrime strategies which implies that guardianship have influence on victimization.

Bossler and Holt (2010) examined data from a self-report survey administered to 788 college students enrolled in southeastern university; they operationalized physical guardianship through an additive scale asking respondents whether they used protective software, updated their operating system, or used a firewall. Their findings yielded no significant relationship between physical guardianship online and malware infection (Bossler & Holt 2010). Also, Choi (2008) found a strong negative relationship between physical guardianship and victimization.

Conceptual Framework Revisited

The framework identified main factors that influence the perceived vulnerability of inbound tourists on cybercrime in Ghana, which included respondents' awareness on cybercrime, their socio demographic features and their travel characteristics. However, the result of the study revealed that not all the variables in the various concepts in the framework have influence on perceived vulnerability. In this end, the main factors that were found to have effect on perceived vulnerability are respondents' level of education and awareness on cybercrime. From the conceptual framework (CF) also, factors influencing victimization were identified to be respondents' awareness on cybercrime, their socio demographic features, their travel characteristics, perceived vulnerability and routine online activities. Again, the study identified awareness, trip experiences (first timers or repeat visitors), purpose of visitation and perceived vulnerability as the factors that influence cybercrime victimization.

In the same way, only perceived vulnerability and cybercrime experiences were identified in the study as factors influencing the choice of online guardianship/preventive strategies. Meanwhile, the framework proposed that it is travel characteristics, socio demographics, awareness, perceived vulnerability and routine online activities that have influence on the adoption of preventive strategies. Again, the framework also proposed that the routine online activities of respondents’ could be influenced by factors such as travel characteristics, socio demographics, awareness and perceived vulnerability. However, the findings proved otherwise. Concerning the coping strategies, the proposed CF failed to include factors that influence the effectiveness of the chosen strategy such as time and type of strategy adopted. Thus, the period or time in which the respondents started using the said strategy and the type of strategy could easily influence victimization if the right strategy is not used. In view of this, the conceptual framework is reconstructed to reflect the findings of the study as shown in Figure 16.

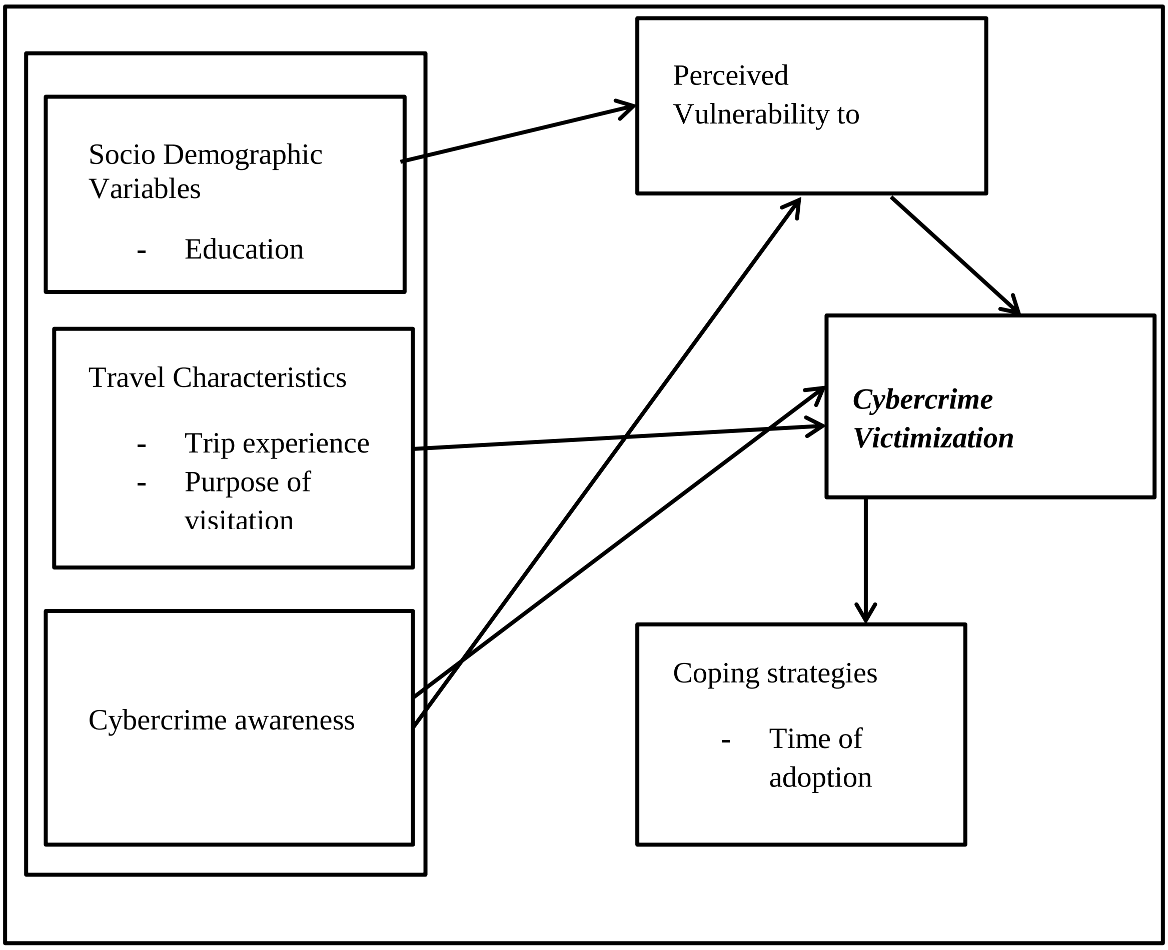

Figure 16: Revised conceptual framework, authors own construct on the perceived vulnerability and experiences of cybercrime, adapted from Cohen and Felson 1979.

CHAPTER FIVE

SUMMARY, CONCLUSIONS AND RECOMMENDATIONS

Introduction

This section is the conclusion chapter of the study. It presents a summary of the thesis including the major findings. It is followed by conclusions drawn based on the main findings. Also, recommendations were made towards cyber security measures for inbound tourists in Ghana as well as avenue for future research.

Summary of Thesis

The main objective of the study was to examine the perceived vulnerability of inbound tourists' on cybercrime in Ghana. The specific objectives of the study were:

- Examine the perceived vulnerability of inbound tourists on cybercrime in Ghana.
- Analyze how tourists' perceived vulnerability on cybercrime shapes their travel decisions.
- Analyze international tourists' experiences on cybercrime in Ghana.
- Explore international tourists' preventive mechanisms on cybercrime.
- Explore the relationship between respondents' background characteristics and their perceived vulnerability to cybercrime.

Based on the objectives of the study, a conceptual framework was adopted from victimization theory by Cohen and Felson (1979). Thus, the Routine Activities Theory (RAT) which holds that crime occurs at the intersection of a motivated offender, a suitable target, and the lack of a capable guardian. The framework captured the main issues based on the objectives of the study which included target suitability, victimization and online capable guardianship on cybercrime.

The study adopted a cross sectional study design and a quantitative approach to data collection and analysis. A total of 370 respondents were selected for the survey using self-administered questionnaires through the use of convenience sample technique. The collected data was edited, coded and analyzed with the help of IBM SPSS v.21. Descriptive statistics were mainly employed in analyzing the quantitative data. Further, chi-square test of independence was also employed to explore the significant relationship between; perceived vulnerability of inbound tourists and cybercrime victimization by their socio demographic and travel characteristics.

Summary of Main Findings

The findings of the study indicate that perceived vulnerability of inbound tourists on cybercrime in Ghana is low. This is because the findings revealed that only a little over one quarter of the respondents (28.6%) indicated that they felt vulnerable to cybercrime in Ghana. Surprisingly, it came out that, respondents perceived other tourists to be more vulnerable to cybercrime than they perceived themselves.

Furthermore, the study observed that, not all inbound tourists include the issue of cybercrime in their travel decisions. This is because, only 69.7 percent of the respondents expressed to have been considering cybercrime issue whenever they are planning a tour to other countries. Notwithstanding, about ten percent (10.6%, n=38) of these respondents (those who include cybercrime issues in their travel decisions, 69.7%, n=258) claimed to have rejected a particular destination or the other in relation to the issue of cybercrime. The remaining 89.7 percent of the respondents said they have not rejected any destination based on the rate or history of its cybercrime issues.

It also emerged from the study that the actual cybercrime experiences of inbound tourists was also quite low (n=39, 10.5%). As well, tourists views on other tourists victimization also appeared to be low (n=50, 13.5%). The forms of cybercrime experienced by these tourists were fraud (credit card, business, advanced fee fraud, romance/dating scam and uber fraud), identity theft and hacking, phishing, and stealing of electronical gadgets.

It is also observed that, a little above half of the respondents 52.2 percent were of the view that, there are ways they can prevent themselves from falling victim to cybercrime. The major preventive strategies shared by the respondents were; the use of strong/complex password (pin, codes, pattern, among others), not sharing personal/financial information with anyone, and avoiding/limiting the use of cards, especially the use of credit cards online and in all your transactions.

Lastly, respondents' level of education was observed to have significant relationship existed between trip experiences, purpose of visitation and respondents cybercrime victimization. Also, respondents' level of education was found to have significant relations with respondents' perceived vulnerability to cybercrime.

Conclusion

Based on the specific objectives and the findings observed, this study offers a number of conclusions that add to literature on perceived vulnerability and victimization of inbound tourists on cybercrime in Ghana.

The study therefore concludes that;

Inbound tourists perceived vulnerability to cybercrime is quite low. Also, the perceived invulnerability of inbound tourists on cybercrime in Ghana is influenced by certain online routine activities or behaviors. Thus, tourists are likely to be invulnerable to cybercrime if tourists; do not use the internet, avoid the use of credit cards and rather focused solely on the use of physical cash in all their purchases, avoid online purchases, avoid the use of unprotected Wi-Fi, and have good computer, phone and internet security. It is concluded that, respondents who considered others to be highly vulnerable than themselves were those who got victimized the most.

Again, it can be concluded that, inbound tourists that visit Ghana do consider the issue of cybercrime when planning for their trip meanwhile their rejection of Ghana as a safe destination for other alternative destinations have never been on the issue of cybercrime. Thus, tourists do not reject their preferred destination as a result of its cybercrime prevalence.

On the whole, it can be established that, although literature has established the fact that cybercrime is on the rise within the borders of Ghana meanwhile, the study observed victimization on inbound tourists to be quite low. Thus, aside tourists own experiences on cybercrime, respondents' views on other tourists' victimization were also found to be low. It is therefore not out of place to conclude that cybercrime victimization of inbound tourists is on the low.

Again, conclusions could be made that inbound tourists agreed on the existence of preventive strategies to cybercrime and are also well aware of what constitute these preventive strategies in limiting their likelihood of falling victim.

Lastly, trip experiences and purpose of visitation have significant association with respondents' cybercrime victimization whereas respondents' level of education also has significant relationship with respondents' perceived vulnerability to cybercrime.

Recommendations

Based on the main findings and conclusions drawn, the following recommendations are made:

Although perceived vulnerability and actual experiences happened to be low but the continuous development and evolvement of new technologies calls for different forms of cybercrime and so awareness on the issue will help tourists keep abreast with it. There should be government developed awareness programs, including TV, radio, internet ads, etc. on the impact of cybercrime which could include testimonials from victims and short case studies that outline some high-profile cases.

It is also recommended that, based on the suggested preventive strategies shared by the tourists, the information should be accessible by all travelers in all possible platforms such as GTA website and on the brochures which could help them to be security conscious and also have the knowledge about the different forms of the said crimes and how the cyber criminals carry out their heinous activities, thus they can devise means of protecting their information from cyber criminals. That is, adoption of preventive strategies should be encouraged.

As suggested by some of the survey responses, majority of the victimized tourists refused to report their experiences to the police or the rightful authorities. It is recommended that, the victimized tourists must be encouraged to share their experiences so as to help the C.I.D have fair idea of the actual cybercrime experiences being faced by the foreign tourists. This practice will also help so that, the cyber criminals will be punished for their wrongdoing.

Suggestions for Future Research

Regarding direction for future research, the following areas could be considered;

This study mainly examined the perceptions and experiences of cybercrime in Ghana with the specific emphases on inbound tourists. However, due to time and logistical constraints, the scope of the research was scaled-down to 370 respondents which limit its general applicability to the larger population. The study can be replicated by considering a large group of people to be able to determine the quantum of its effects.

This study also focused on quantitative approach of data collection and analysis. To be able to obtain more insightful study of visitors' experiences on cybercrime, the qualitative or the mixed method approach could be adopted. Further studies could also be conducted to find out how the scammers successfully defrauded them but with this, the researcher could probe further if qualitative method is adopted.

One possible avenue of research could focus on empirical research around behavior online. This is an important aspect of the problem and further research is required. An exploration of the legislation and legal precedents that exist in the area of cybercrime in Ghana might be very instructive in terms of how it handles reports of international tourists on their cybercrime experiences.

REFERENCES

Abem, E. C. (2013). *Combating Cybercrime in Ghana: Prospects and Challenges* (Doctoral dissertation, University of Ghana).

Adam, I. (2015). Backpackers' risk perceptions and risk reduction strategies in Ghana. *Tourism Management*, *49*, 99-108.

Adam, I., & Adongo, C. A. (2016). Do backpackers suffer crime? An empirical investigation of crime perpetrated against backpackers in Ghana. *Journal of Hospitality and Tourism Management*, *27*, 60-67.

Aidoo, D., Akotoye, F., & Ayebi-Arthur, K. (2012). Academic 419: Locating computer crime in the use of ICT for management of educational system in Ghana- The case of University of Cape Coast. *Journal of Educational Management*.

Allen, J. (1999). Crime against international tourists. *BOCSAR NSW Crime and Justice Bulletins*, 8.

Alpna, S., Malhotra, (2016). DDOS Attack Detection and Prevention Using Ensemble Classifier (Random Forest). [Accessed 20 September 2018] Availableat:https://www.ijarcsse.com/docs/papers/Volume6/6_June2018/V6I6-0375.pdf.

Alshalan, A. (2006). *Cyber-crime fear and victimization: An analysis of a national survey*.

Amissah, E. F. (2013). Tourist satisfaction with hotel services in Cape Coast and Elmina, Ghana. *American Journal of Tourism Management*, *2*(1), 26-33.

Anderson, D. J. (2010). *Kanban: successful evolutionary change for your technology business*. Blue Hole Press. Attitude towards hotels in Accra. *International Journal of Academic Research in Business and Social Sciences, 3*(5), 444.

Attitude towards hotels in Accra. *International Journal of Academic Research in Business and Social Sciences, 3*(5), 444.

Audit Commission for Local Authorities in England and Wales. (1998). *Ghost in the machine: an analysis of IT fraud and abuse*. Audit Commission.

Avais, M. A., Wassan, A. A., Narejo, H., and Khan, J.A., 2014. Awareness Regarding Cyber Victimization among Students of University of Sindh, Jamshoro. *International Journal of Asian Social Science*. 4(5): 632-641

Ayeh, J. K. (2015). Ghana, tourism.

Ayofe, A. N., & Oluwaseyifunmitan, O. S. U. N. A. D. E. (2009). Towards ameliorating cybercrime and cybersecurity. *International Journal of Computer Science and Information Security*, *3*, 1-11.

Baker, D. M. A., & David (2014). The effects of terrorism on the travel and tourism Industry. *International Journal of Religious Tourism and Pilgrimage*, *2*(1), 9.

Baker, D., & Stockton, S. (2014). Tourism and Crime in America: A Preliminary Assessment of the Relationship between the Number of Tourists and Crime in two Major American Tourist Cities. *IJSSTH*, *1*(5), 1-25.

Barfi, K. A., Nyagorme, P., & Yeboah, N. (2018). The internet users and cybercrime in Ghana: Evidence from senior high school in Brong Ahafo Region. *Library Philosophy and Practice*, p.1-16.

Barrett, M., Steingruebl, A., & Smith, B. (2011). Combating cybercrime: Principles, policies, and programs.

Biztechafrica.com (2014, July 8). *Cybercrime issues in Ghana; Government have run out of ideas on how to tackle cybercrime.*

Boakye, K. A. (2010). Studying tourists' suitability as crime targets. *Annals of Tourism Research*, *37*(3), 727-743.

Boakye, K. A. (2012). Tourists' views on safety and vulnerability. A study of some selected towns in Ghana. *Tourism Management*, *33*(2), 327-333.

Boateng, R., Longe, O. B., Mbarika, V., Avevor, I., & Isabalija, S. R. (2010, August). Cyber Crime and Criminality in Ghana: Its Forms and Implications. In *AMCIS* (p. 507).

Boateng, R., Olumide, L., Isabalija, R. S., & Budu, J. (2011). Sakawa-cybercrime and criminality in Ghana. *Journal of Information Technology Impact*, *11*(2), 85-100.

Bokpe, S. J. (2013). A project to promote transparency in public procurement unveiled daily graphic. Available from http://www.graphic.com.gh/news/generalnews/16339-project-to-promote-transparency-in-public-procurementunveiled.html

Bossler, A. M., & Holt, T. J. (2009). On-line activities, guardianship, and malware infection: An examination of routine activities theory. *International Journal of Cyber Criminology*, *3*(1).

Bossler, A. M., & Holt, T. J. (2010). The effect of self-control on victimization in the cyberworld. *Journal of Criminal Justice, 38*(3), 227-236.

Breda, Z., & Costa, C. (2006). Safety and security issues affecting inbound tourism in the People's Republic of China. *Tourism, Security and Safety, from theory to practice*, 187-208.

Britz, M. T. (2008). Computer Forensic and Cyber Crime.

Britz, M. T. (2009). *Computer Forensics and Cyber Crime: An Introduction, (2nd-ed)*. Pearson Education India.

Brunt, P., & Shepherd, D. (2004). The influence of crime on tourist decision-making: Some empirical evidence in *Tourism (13327461)*, *52*(4).

Brunt, P., Mawby, R., & Hambly, Z. (2000). Tourist victimization and the fear of crime on holiday. *Tourism Management*, *21*(4), 417-424.

Bryman, A. (2008). Social Research Methods (3rd. ed.). New York: Oxford University Press.

Buhalis, D., & Deimezi, O. (2003). Information technology penetration and E-commerce Developments in Greece, with a focus on small to medium sized Enterprises. *Electronic Markets*, *13*(4), 309-324.

Buhalis, D., & Law, R. (2008). Progress in information technology and tourism management: 20 years on and 10 years after the Internet—The state of Tourism research. *Tourism Management*, *29*(4), 609-623.

Burns, N., & Grove, S. K. (1993). Advanced statistical analyses. *The practice of nursing research. Conduct, critique and utilization*, 605-629.

Button, M., Nicholls, C. M., Kerr, J., & Owen, R. (2014). Online frauds: Learning from victims why they fall for these scams. *Australian & New Zealand Journal of Criminology*, *47*(3), 391-408.

Center for Strategic and International Studies (2017). Net Losses: Estimating the Global Cost of Cybercrime, Santa Clara: Mcafee, http://www.mcafee.com/ca/resources/reportseconomic-impact.

Chawki, M. (2009). Nigeria tackles advance fee fraud. *Journal of Information, Law and Technology*, *1*(1), 1-20.

Chen, J., Paik, M., & McCabe, K. (2014). Exploring internet security perceptions and practices in urban Ghana. In *10th Symposium on Usable Privacy and Security ({SOUPS} 2014)* (pp. 129-142).

Choi, K. S. (2008). Computer crime victimization and integrated theory: An empirical assessment. *International Journal of Cyber Criminology*, *2*(1).

Clark, C. (2015). The Serious cyber security threat that could hurt hotels. Retrieved February 26, 2016, from http://www.pcma.org/news/news-landing/2015/04/13/the-serious-cyber-security-threat-that-could-hurt-hotels#.

Cobanoglu, C., & Demicco, F. J. (2007). To be secure or not to be: Isn't this the question? A critical look at hotel's network security. *International Journal of Hospitality & Tourism Administration*, *8*(1), 43-59.

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review*, 44, 588-608.

Colin R., Emily J. S., (2018). Police use of technology: insights from the literature. *International Journal of Emergency Services*, Vol. 7 Issue: 2, pp.100-110, https://doi.org/10.1108/IJES-03-2018-0012

Computer Security Institute, (2001). CSI/FBI Computer Crime and Security Survey, *Computer Security Issue & Trends*, vol. 7 (1), pp. 1–20.

Coomson, J. (2006). Cybercrimes in Ghana. *Ghanaian Chronicle, 4*.

Copes, H., Kerley, K. R., Huff, R., & Kane, J. (2010). Differentiating identity theft: An exploratory study of victims using a national victimization survey. *Journal of Criminal Justice*, *38*(5), 1045-1052.

Cox, C., Burgess, S., Sellitto, C., & Buultjens, J. (2009). The role of user-generated content in tourists' travel planning behavior. *Journal of Hospitality Marketing & Management*, *18*(8), 743-764.

Cunningham, L. F., Gerlach, J. H., Harper, M. D., & Young, C. E. (2005). Perceived risk and the consumer buying process: internet airline reservations. *International Journal of Service Industry Management*, *16*(4), 357-372.

Daily Graphic (2013, April 15). *Ghana second in Africa in terms of cybercrime.* P.7

Danquah, P., & Longe, B. (2011). Cyber deception and theft: An ethnographic study on cyber criminality from a Ghanaian perspective. *Journal of Information Technology Impact* 11(3) 169-182.

Das, S., & Nayak, T. (2013). Impact of cybercrime: Issues and challenges. *International Journal of Engineering Sciences & Emerging technologies*, *6*(2), 142-153.

Dashora, K. (2011). Cybercrime in the society: Problems and preventions. *Journal of Alternative Perspectives in the Social Sciences*, *3*(1), 240-259.

Dayour, F. (2013). Motivations of backpackers in the Cape Coast-Elmina conurbation, Ghana.

Dayour, F., & Adongo, C. A. (2015). Why they go there: International tourists' motivations and revisit intention to Northern Ghana. *American Journal of Tourism Management*, *4*(1), 7-17.

Dayour, F., Kimbu, A. N., & Park, S. (2017). Backpackers: The need for reconceptualization. *Annals of Tourism Research*, *66*, 191-193.

Dayour, F., Park, S., & Kimbu, A. N. (2019). Backpackers' perceived risks towards smartphone usage and risk reduction strategies: A mixed methods study. *Tourism Management*, *72*, 52-68.

De Vaus, D. (2002). Analyzing social science data*: 50 key problems in data analysis*. Sage.

Dei Mensah, R., & Mensah, I. (2013). *Management of tourism and hospitality services*. Xlibris Corporation.

Dimc, M., & Dobovšek, B. (2010). Perception of cybercrime in Slovenia. *Varstvoslovje, Journal of Criminal Justice and Security*, (4) 378-396.docs/reports/2016-norton-cyber-security-insightsreport.pdf

Duah, F. A., & Kwabena, A. M. (2015). The impact of cybercrime on the development of electronic business in ghana. *European Journal of Business and Social Sciences*, *4*(01), 22-34.

Duggal, P. (2015). Cyber security law. New Delhi: Saakshar Law Publications.

Ennin, D. A. N. I. E. L. (2015). *Cybercrime in Ghana. A Study of Offenders, Victims and the Law* (Doctoral dissertation, University of Ghana). Ferraro, K. F., & Grange, R. L. (1987). The measurement of fear of crime. *Sociological inquiry*, *57*(1), 70-97.

Frimpong, O. J. (2011). Sakawa: on occultic rituals and cyberfraud in Ghanaian popular cinema. línea:] http://www. media-anthropology. net/file/ frimpong_ rituals_cyberfraud. pdf.(Consultado el 18 de noviembre de 2017).

Furnell, S. M. (2001). The problem of categorizing cybercrime and cybercriminals. In *Australian Information Warfare and Security Conference 2001*.

Ganzini, L., McFarland, B., & Bloom, J. (1990). Victims of fraud: Comparing victims of white collar and violent crime. *Journal of the American Academy of Psychiatry and the Law Online*, *18*(1), 55-63.

Garrett, E. V., (2014). Exploring internet user vulnerability to online dating fraud: Analysis of routine activities theory factors.

George, L. K. (2003). Life course research. In *Handbook of the life course* (pp. 671-680). Springer, Boston, MA.

George, R. (2010). Visitor perceptions of crime-safety and attitudes towards risk: The case of Table Mountain National Park, Cape Town. *Tourism Management*, *31*(6), 806-815.

Ghana Business News, (2010, 15 December). Ghana, Nigeria cited among top 10 countries where cybercrime is most prevalent. Ghanaweb

Ghana Business News, (2018, Oct 26th, Tue). Awareness creation on Cybercrime key for digital migration. Ghanaweb

Ghana general news (2013, August). Ghana ranks third in Africa in terms of cybercrime, Ghanaweb news.

Ghana General News (2017, March 20). The case of cyber fraudsters caught in Alhaji Tabora, Ghanaweb news.

Ghana general news. (2014). Cybercriminals who got caught at Adabraka, a suburb in Accra.

Ghana Police Service, Director of cybercrime unit (2018, October 11). *The rate of cybercrime in Ghana.* Ghanaweb Business news.

Ghana Tourism Authority, (2014). Tourism fact sheet. Ghana: Author.

Giddens, A. (1990). Sociology, 2nd Edition, Cambridge, Blackwell, Publishers.

Goodman, M. (2001). Making Computer Crime Count, FBI Law Enforcement Bulletin. P. 10-17.

Gordon, G. R., Hosmer, C. D., Siedsma, C., & Rebovich D., (2004). Assessing technology, methods, and Information for committing and combating cybercrime.

Grabosky, P. (2001).Virtual criminality: Old wine in new bottles? *Social and Legal Studies*, 10, 243-249.

Gretzel, U., & Jamal, T. (2009). Conceptualizing the creative tourist class: Technology, mobility, and tourism experiences. *Tourism Analysis*, *14*(4), 471-481.

Grimes, G. A., Hough, M. G., Mazur, E., & Signorella, M. L. (2010). Older adults' knowledge of internet hazards. *Educational Gerontology*, *36*(3), 173-192.

Gurjar, S., Baggili, I., Breitinger, F., & Fischer, A. (2015). An Empirical Comparison of Widely Adopted Hash Functions in Digital Forensics: Does the Programming Language and Operating System Make a Difference?

Halevi, T., Lewis, J., & Memon, N. (2013). A pilot study of cyber security and privacy related behavior and personality traits. In *Proceedings of the 22nd International Conference on World Wide Web* (pp. 737-744). ACM.

Haque, S. I., & Rahman, M. A. (2012). E-Commerce in India: Issues & Remedies. *Business Spectrum, 13*.

Hasan, M. S., Rahman, R. A., Abdillah, S. F. H. B. T., & Omar, N. (2015). Perception and awareness of young internet users towards cybercrime: Evidence from Malaysia. *Journal of Social Sciences*, *11*(4), 395.

Hassan, A. B., Lass, F. D., & Makinde, J. (2012). Cybercrime in Nigeria: Causes, effects and the way out. *ARPN Journal of Science and Technology*, *2*(7), 626-631.

Henderson, S. J. (2007). *The dark visitor: Inside the world of Chinese hackers*. Lulu. com.

Henson, B., Reyns, B. W., & Fisher, B. S. (2013). Fear of crime online? Examining the effect of risk, previous victimization, and exposure on fear of online interpersonal victimization. *Journal of Contemporary Criminal Justice, 29*(4), 475-497.

Heppner, P. P., Wampold, B. E., & Kivlighan, D. M. (2008). Quantitative descriptive designs. *Research designs in counseling, 3*, 224-255.

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

Holt, T. J., & Bossler, A. M. (2008). Examining the applicability of lifestyle-routine activities theory for cybercrime victimization. *Deviant Behavior*, *30*(1), 1-25.

Holt, T. J., Bossler, A. M., & Seigfried-Spellar, K. C. (2015). *Cybercrime and digital forensics: An introduction*. Routledge p. 309-313.

Information Security Congress, Orlando Florida (2016, September). *Psychological impacts of cybercrime*.

ITU, (2008). ICT statistics [Online] http://www.itu.int/ITUD/ict/statistics/ict/index.html

Jaishankar, K. (2008). Space transition theory of cybercrimes. *Crimes of the Internet*, 283-301.

Kamruzzaman, M., Islam, M. A., Islam, M. S., Hossain, M. S., & Hakim, M. A. (2016). Plight of youth perception on cybercrime in South Asia. *American Journal of Information Science and Computer Engineering*, *2*(4), 22-28.

Kanan, J. W., & Pruitt, M. V. (2002). Modeling fear of crime and perceived victimization risk: The (in) significance of neighborhood integration. *Sociological inquiry*, *72*(4), 527-548.

Kenyan based IT firm (2017) report. Economic impacts of cybercrime. Ghanaweb business news.

Kethineni, S., Cao, Y., and Dodge, C. (2017). Use of Bitcoin in Darknet Markets: Examining facilitative factors on Bitcoin-Related Crimes, *American Journal of Criminal Justice, Springer New York LLC*, pp. 1–17. (https://doi.org/10.1007/s12103-017-9394-6).

Khan, J., Abbas, H., & Al-Muhtadi, J. (2015). Survey on mobile user's data privacy threats and defense mechanisms. *Procedia Computer Science*, *56*, 376-383.

Kim, I., H., Qu, H., & kim, D. J. (2009). A study of perceived risk and risk reduction of purchasing air-tickets online. Journal of Travel and Tourism Marketing, 26(3), 203-224.

Kotler, P., Bowen, J. T., Markens, J. C., (2006). Marketing for hospitality and tourism, New Jersey, Pearson Prentice Hall International Edition.

Kumar, R. (2005) Research Methodology: A step-by-step guide for beginners (2nd ed.). London: Sage Publications.

Kumekpor, T., B., K., (2002). Research Methods and Techniques of Social Research SonLife Printing Press and Services, Adenta Accra.

Kwablah, E. (2009). Cybercrime: Giving a bad name to Ghana. *Business and Financial Times*.

Lan, T., Li, Y., Murugi, J. K., Ding, Y., & Qin, Z. (2018). RUN: Residual U-Net for Computer-Aided Detection of Pulmonary Nodules without Candidate Selection. *arXiv preprint arXiv:1805.11856*.

Leukfeldt, E. R. (2014). Phishing for suitable targets in the Netherlands: Routine activity theory and phishing victimization. *Cyberpsychology, Behavior, and Social Networking*, *17*(8), 551-555.

Leukfeldt, E. R., & Yar, M. (2016). Applying routine activity theory to cybercrime: A theoretical and empirical analysis. *Deviant Behavior* , *37*(3), 263-280.

Levalle, R. (2016). Is the hotel industry serious about cyber security? Retrieved February 26, 2018, from https://www.zenedge.com/blog/is-the-hotel-industry-seriousabout cyber-security

Levitt, S. D. & Lochner, L. (2000). The determinants of juvenile crime risky behavior among youths: An Economic Analysis Chicago: University of Chicago Press, 327-73.

Liddle, A. J. (2003). BK seeks simplification of complex network, online identity management process. *Nation's Restaurant News*, *37*(40), 36-36.

Longe, O., Ngwa, O., Wada, F., Mbarika, V., & Kvasny, L. (2009). Criminal use of Information and Communication Technologies in Sub-Saharan Africa: Trends, Concerns and Perspectives. *Journal of Information Technology Impact*, 9(3), 155-165.

Lynch, J. (2014). The evolving role of self-report surveys of criminal victimization in a system of statistics on crime and the administration of justice. *Statistical Journal of the IAOS*, *30*(3), 165-169.

Magele, T. (2005). E-security in South Africa, White Paper prepared for the Forge Ahead e-Security event. Retrieved October 22, 2009, from www.forgeahead.co.za/

Magliulo, A. (2016). Cyber security and tourism competitiveness. *European Journal of Tourism, Hospitality and Recreation*, *7*(2), 128-134.

Mansfeld, Y., & Pizam, A. (Eds.). (2006). *Tourism, security and safety*. Routledge.

Marcum, C. D. (2008). Identifying potential factors of adolescent online victimization for high school seniors. *International Journal of Cyber Criminology*, *2*(2).

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

Mawby, R. I. (2000). Tourists' Perceptions of Security: The Risk—Fear Paradox. *Tourism Economics*, *6*(2), 109-121.

McAfee, (2014). Net Losses: Estimating the global cost of cybercrime, Economic Impact of Cybercrime II, Center for Strategic and International Studies.

McGuire, M., & Dowling, S. (2013). Cybercrime: A review of the evidence. *Summary of key findings and implications. Home Office Research report, 75*.

Meier, R. F., & Miethe, T. D. (1993). Understanding theories of criminal v ictimization. *Crime and Justice*, *17*, 459-499.

Meke, E. S. N. (2012). Urbanization and Cyber Crime in Nigeria: Causes and Consequences. *European Journal of Computer Science and Information Technology*, *3*(9), 1-11.

Merrit, J. (2007). An appetite for travel. Travel Agent, 328(11) 20-23.

Mest, E. (2015). Fake booking websites and the tangled web they weave. Retrieved February 28, 2018, from http://www.hotelmanagement.net/ technology/fake-booking websites- and-the-tangled-web-they-weave-32968

Ministry of Communication (2018, October 22). *The introduction of mobile money and its impacts individuals' in terms of fraud.* Ghana Business News.

Ministry of National Security (2017, April 4). *Cybercrime issues in Ghana*. General news on myjoyonline.com

Ministry of Tourism, (2015). *Ghana tourism Statistics.* Accra, Ghana

Modic, D. (2012). Willing to be scammed: How self-control impacts Internet scam compliance.

Morrison, A. M. (2013). *Marketing and managing tourism destinations*. Routledge.

Muscat, G., Graycar, A., & James, M. P. (2002). *Older people and consumer fraud*. Canberra: Australian Institute of Criminology.

Myjoyonline.com. (2013, July 21). Cybercrime: Ghana 2nd in Africa, 7th in the world. Retrieved February 07, 2017, from Myjoyonline.com: http:// edition.myjoyonline.com/pages/news/201307/110530.php

Nakashima, E., & Peterson, A. (2014). Report: Cybercrime and espionage costs $445 billion annually. The Washington Post.

National Communications Minister (2018, October 26). *The fight against cybercrime. Ghanaweb general news.*

National White-Collar Crime Center (2002) Internet Fraud Report: January 1, 2002- December 31, 2002. http://www.ifccfbi.gov/strategy/2002_ IFCC Report.pdf.

Nayak, H. (2016). Impact of cybercrime on tourism industry. *International Journal in Management & Social Science*, *4*(4), 160-174.

Neuman, L. W. (2007). *Social Research Methods, 6/E*. Pearson Education India.

Ngo, F. T., & Paternoster, R. (2011). Cybercrime victimization: An examination of individual and situational level factors. *International Journal of Cyber Criminology,* 5(1), 773.

Noone, F. (2015, August 05). Defending Against Cyber-Security Threats in Your Hotel Room - ECC IT Solutions.

Norton cyber security insight report (2018): *Understanding cybercrime and the consequences of constant connectivity*. Global economic impacts of cybercrime.

O'Connor, P. (1999). *Electronic information distribution in tourism and hospitality*. CAB international.

Okeshola, F. B., & Adeta, A. K. (2013). The nature, causes and consequences of cybercrime in tertiary institutions in Zaria-Kaduna state, Nigeria. *American International Journal of Contemporary Research*, *3*(9), 98-114.

Olding, A., & Turner, P. (2007). Cyber vulnerabilities and the tourism industry: developing a conceptual framework. *ACIS 2007 Proceedings*, 116.

Osei-Bryson, K. M., & Ngwenyama, O. (2014). An approach for using data mining to support theory development. In *Advances in Research Methods for Information Systems Research* (pp. 23-43). Springer, Boston, MA.

Park, S., & Tussyadiah, I. P. (2017). Multidimensional facets of perceived risk in mobile travel booking. *Journal of Travel Research*, *56*(7), 854-867.

Pati, P. (2003). Cybercrime, New Delhi.

Pehlivan, R., Yüksel, F., & Yuksel, A. (2007). Perceived risks: A comparison between types of daily trips bought from local tour agencies whilst on vacation. *Journal of Travel & Tourism Research*, *7*(1).

Pereira, F., Spitzberg, B. H., & Matos, M. (2016). Cyber-harassment victimization in Portugal: Prevalence, fear and help-seeking among adolescents. *Computers in Human Behavior*, *62*, 136-146.

Pizam, A., & Mansfeld, Y. (1996). *Tourism, crime, and international security issues*. John Wiley & Son Ltd.

Poon, A. (1993). *Tourism, technology and competitive strategies*. CAB international.

Pratt, T. C., Holtfreter, K., & Reisig, M. D. (2010). Routine online activity and internet fraud targeting: Extending the generality of routine activity theory. *Journal of Research in Crime and Delinquency*, *47*(3), 267-296.

Price water house Coopers, L. L. P. US cybercrime: Rising risks, reduced readiness Key findings from the 2014 US State of Cybercrime Survey.

Reingold, D. A. (1999). Social Networks and the Employment Problem of the Urban Poor'. Urban Studies, Vol. 36, No. 11, pp. 1907–32.

Reyns, B. W., Henson, B., & Fisher, B. S. (2011). Being pursued online: Applying cyber lifestyle–routine activities theory to cyberstalking victimization. *Criminal Justice and Behavior*, *38*(11), 1149-1169

Roberts, L. D. (2009). Cyber-victimization. In *Handbook of research on technoethics* (pp. 575-592). IGI Global.

Roberts, L. D., Indermaur, D., & Spiranovic, C. (2013). Fear of cyber-identity theft and related fraudulent activity. *Psychiatry, Psychology and Law*, *20*(3), 315-328.

Salvador, W. J. (2015). Dismantling the Internet Mafia: RICO's Applicability to Cyber Crime. *Rutgers Computer & Tech. LJ*, *41*, 268.

Scammers in E-Harmony.com (2011). Ghana and Nigerian, the most frequenting nationalities behind America and Britons attack.

Schiebler, S. A., Crotts, J. C., & Hollinger, R. C. (1996). Florida tourists' vulnerability to crime. *Tourism, crime and international security issues*, 37-50.

Schoepfer, A., & Piquero, N. L. (2009). Studying the correlates of fraud victimization and reporting. *Journal of Criminal Justice*, 37(2), 209-215

Shabani, N. (2017). A study of cyber security in hospitality industry-threats and countermeasures: case study in Reno, Nevada. *arXiv preprint arXiv:1705.02749*.

Shehu, Y. A. (2014). Emerging issues in Cybercrime: Causes, implications and effects for the Legal Profession. *Online Journal of Social Sciences Research*, 3 (7), pp 169-180.

Sheng, S., Holbrook, M.B., Kumaraguru, P., Cranor, L.F., and Downs, J.S. (2010). Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions. In *Proceedings of the CHI Conference on Human Factors in Computing Systems* (Atlanta, Apr. 10–15). ACM Press, New York, 2010, 373–382.

Stanko, E. A. (2000). Victims R us. *Crime, risk and insecurity: Law and order in everyday life and political discourse*, 13-30.

Stephure, R. J., Boon, S. D., MacKinnon, S. L., & Deveau, V. L. (2009). Internet initiated relationships: Associations between age and involvement in online dating. *Journal of Computer-Mediated Communication*, *14*(3), 658-681.

Symantec, N. (2016). Norton Cyber Security Insights Report 2016. *Nort. Symantec*, 3-9

Tarlow, P. E. (2006). Crime and tourism. In *Tourism in turbulent times* (pp. 117-130). Routledge.

Tarlow, P. E. (2009). Tourism safety and security. *The SAGE handbook of tourism studies*, 464-480.

Ten, C. W., Liu, C. C., & Manimaran, G. (2008). Vulnerability assessment of cybersecurity for SCADA systems. *IEEE Transactions on Power Systems*, *23*(4), 1836-1846.

The Ghanaian Times (2012, June 4). *Cybercrime growth in Ghana and Cybercrime perpetration in Ghana*. p.8

Thompson, K. (1979). PaSSWOrd Security; a Case history. *Communications of the ACM*, *22*.

Timothy, D. J., & Butler, R. W. (1995). Cross-boder shopping: A North American perspective. *Annals of tourism research*, *22*(1), 16-34.

Titus, R. M. (1999). The victimology of fraud. In *Restoration for Victims of Crime Conference, Australian Institute of Criminology, Melbourne, Australia*.

Trahan, A., Marquart, J. W., & Mullings, J. (2005). Fraud and the American dream: Toward an understanding of fraud victimization. *Deviant Behavior*, *26*(6), 601-620.

Trust Wave Global Security Report (2012). *The Hospitality and Tourism industry ranked at the top of the list of security breaches*.

Tussyadiah, I. P., & Zach, F. J. (2012). The role of geo-based technology in place experiences. *Annals of Tourism Research*, *39*(2), 780-800.

U.S Federal Bureau of Investigation (FBI). (2015). Safety and security for US students travelling abroad. Retrieved from http://:www.state.gov/travel

United Kingdom Foreign and Commonwealth Office Travel Advisory (2015). Foreign travel advice. Retrieved 18 April 2018, from www.gov.uk/ foreign-travel-advice/ghana/ safety-and-security.

United Nations World Tourism Organization (UNWTO) (2011). UNWTO Tourism Highlights (2011). Madrid: UNWTO.

Valkenburg, P. M., & Peter, J. (2007). Online communication and adolescent well-being: Testing the stimulation versus the displacement hypothesis. *Journal of Computer-Mediated Communication*, *12*(4), 1169-1182.

Van Wilsem, J. (2011). Worlds tied together? Online and non-domestic routine activities and their impact on digital and traditional threat victimization. *European Journal of Criminology*, *8*(2), 115-127.

Van Wyk, J., & Mason, K. A. (2001). Investigating vulnerability and reporting behavior for consumer fraud victimization: Opportunity as a social aspect of age. *Journal of Contemporary Criminal Justice*, *17*(4), 328-345.

Walsham, G. (1995). The emergence of interpretivism in IS research. *Information Systems Research*, *6*(4), 376-394.

Wang, D., Park, S., & Fesenmaier, D. R. (2012). The role of smartphones in mediating the touristic experience. *Journal of Travel Research*, *51*(4), 371-387.

Wang, Q. H., & Kim, S. H. (2009). Cyber-attacks: Does physical boundary matter? AIS.

Warner, J. (2011). Understanding cyber-crime in Ghana: A view from below. *International Journal of Cyber Criminology*, *5*(1), 736.

Whitty, M., & Buchanan, T. (2012). The psychology of the online dating romance scam. *A report for the ESRC. In*, 23.

Williams, M. L. (2015). Guardians upon high: An application of routine activities theory to online identity theft in Europe at the country and individual level. *British Journal of Criminology*, *56*(1), 21-48.

World Tourism and Travel Council (WTTC) (2017). Tourism: Global Economic Impact & Issue 2018. *WTTC: London, UK*.

World Travel and Tourism Council. (2018). WTTC data gateway. Retrieved from http://www.wttc.org/datagateway/.

Wright, R. T., & Marett, K. (2010). The Influence of Experiential and Dispositional Factors in Phishing: An Empirical Investigation of the Deceived. *Journal of Management Information Systems*, *27*(1), 273–303. doi:10.2753/MIS0742-1222270111

Yamane, T., (1967), Elementary Sampling Theory, New Jersey: Prentice-Hall, Inc.

Yar, M. (2005). The Novelty of 'Cybercrime' An Assessment in Light of Routine Activity Theory. *European Journal of Criminology*, *2*(4), 407-427.

Yassir, A., & Nayak, S. (2012). Cybercrime: a threat to network security. *International Journal of Computer Science and Network Security (IJCSNS)*, *12*(2), 84.

Yu, S. (2014). Fear of cybercrime among college students in the United States: An exploratory study. *International Journal of Cyber Criminology*, *8*(1).

Yuan, Y. L., Gretzel, U., & Fesenmaier, D. R. (2006). The role of information technology use in American convention and visitors bureaus. *Tourism Management*, *27*(2), 326-341.

Zhang, C., & Prichard, J. J. (2009). An empirical study of cyber security perceptions, awareness and practice. *Issues in Information System*, 242-248.

APPENDIX
UNIVERSITY OF CAPE COAST

DEPARTMENT OF HOSPITALITY AND TOURISM MANAGEMENT

QUESTIONNAIRE FOR INTERNATIONAL TOURISTS

Dear sir/madam,

The focus of this study is to examine the perceived vulnerability and experiences of inbound tourists in Ghana and it is in connection with an MPhil Thesis as part of the requirements for an award of a degree. The study is purely for academic purposes and so the researcher will be most grateful for your contribution in this study by completing this questionnaire. All information provided is for academic purposes and therefore your anonymity and confidentiality is assured. Thank you for your co-operation.

MILLICENT DADSON milliesidadson91@gmail.com (02058682320)

SECTION A: PERCEPTIONS OF TOURISTS' ON CYBER VULNERABILITY IN GHANA

Instructions: please tick [ ] or fill the blank spaces where applicable

1. What do you understand by cybercrime?

   …………………………………………………………………………………
   …………………………………………………………………………………
   …………………………………………………………………………………

2. Have you heard of any incidents of cybercrime in Ghana?

   1. Yes [ ] 2. No [ ]

3. If yes, which form(s) of cybercrime have you heard is prevalent in Ghana

   …………………………………………………………………………………
   …………………………………………………………………………………

4. What are your sources of information on cybercrime in Ghana

1. News/media reports [ ] 3. Friends and family [ ]

2. Internet [ ] 4. Others specify………………………

5. In what ways do you think people become vulnerable to cybercrime in Ghana?

....

....

6. Do you consider yourself to be vulnerable to cybercrime in Ghana?

1. Yes [ ] 2. No [ ]

Please explain your answer……………………………………………………

………………………………………………………………………………..

7. Do you think other tourists are vulnerable to cybercrime in Ghana?

1. Yes [ ] 2. No [ ]

Please explain your answer…………………………………………………

………………………………………………………………………………

………………………………………………………………………………

SECTION B: HOW TOURISTS KNOWLEDE ON CYBERCRIME INFLUENCES THEIR TRAVEL DECISIONS

8. Do you consider cybercrime issues before travelling to a particular destination?

1. Yes [ ] 2. No [ ]

9. Have you ever rejected a particular destination as a result of its cybercrime rate?

1. Yes [ ] 2. No [ ]

10. Which of the following devices did you travel to Ghana with?

1. Smartphone [ ]

2. Credit card [ ]

3. Laptops [ ]

4. Hard drives [ ]

5. Ipads, Kindle, Samsung [ ]

6. Others please specify……………………………………………………..

11. Do you use the internet during your stay in Ghana? 1. Yes [ ] 2. No [ ]

12. Which devices do you use for accessing the Internet the most?

………………………………………………………………………………….

13. What is your main purpose for using the Internet whilst in Ghana? Please tick as many as applicable.

1. Leisure (TV, Movie, Music) [ ] 4. News/news articles [ ]

2. Information search/study [ ] 5. Chatting [ ]

3. Online shopping [ ] 6. Other………………………….

SECTION C: TOURISTS EXPERIENCES ON CYBERCRIME

14. Have you personally been a victim to any form of cybercrime in Ghana? 1. Yes [ ] 2. No [ ]

If yes, please answer 1-11

1. Did you experience it in your home country by a Ghanaian?

1. Yes [ ] 2. No [ ]

2. Did you experience it during your stay in Ghana?

1. Yes [ ] 2. No [ ]

3. What form(s) of cybercrime were you a victim to…………………………

4. How did you become a victim of cybercrime in Ghana?

…………………………...………………………………………………

…..………..……………………...

5. How many times have you been a victim to cybercrime in Ghana…………………….……………………………………………………

6. What did you do when/after you got victimized?

1. I reported it [ ] 3.Other…………………………………….

2. I kept it to myself [ ]

7. Have you ever lost money as a result of cybercrime to Ghanaian perpetrators?

1. Yes [ ] 2. No [ ]

8. If yes, how much money did you lose?

....

9. Has your being a victim of cybercrime influenced your perception of Ghana as a destination? 1. Yes [ ] 2. No [ ].

Please explain your answer ……………………………………………………

…………………………………………………………………………………..

10. Based on your experiences, will you repeat your visit? 1. Yes [ ] 2. No [ ]

Please explain …………………………………………………………………

…………………………………………………………………………………..

11. Will you recommend Ghana as a safe destination to other tourists?

1. Yes [ ] 2. No [ ]

Please explain…………………………………………………………………

…………………………………………………………………………..

15. Do you know of any tourist(s) who has/have been a victim to cybercrime in Ghana? 1. Yes [ ] 2. No [ ]

1. If yes, what type(s) of cybercrime did the person(s) experienced……………………...

   ....

SECTION D: TOURISTS PREVENTIVE MECHANISMS

16. Do you know that there are preventive measures to cybercrime?

    1. Yes [ ] 2. No [ ]

If yes, answer question 1and 2

1. Which of these preventive measures do you deploy? List as many as applicable.

   ………………………………………………………………………….

   ………………………………………………………………………….

   ………………………. ………………………………….....................

2. Which of the preventive measures listed above are deemed more reliable? ………………………………………………………......

   …………………………………………………………………………..

   …………………………………………………………………………..

SECTION E: SOCIO DEMOGRAPHIC CHARACTERISTICS

17. Country of Origin……………………………………………………...

18. Sex: 1. Male [ ] 2. Female [ ]

19. Age in complete years: ………………………………………………..

20. Religion

    1. Christianity [ ] 3. Islam [ ]
    2. Atheism [ ] 4. Others please specify…………………

21. Highest education level

1. Primary/basic [ ] 4. Post graduate [ ]
2. High school/ secondary [ ] 5. Other, specify………………
3. College/University [ ]

22. Type of accommodation

1. Hotel [ ]
2. Guest house [ ]
3. Stayed with friends and family [ ]

23. Marital status

1. Single [ ] 3. Divorced [ ]

2. Married [ ] 4. Widowed [ ]

24. Monthly income level

(US$)………………………………………………………………………..

25. Main profession/occupation………………………………………………

SECTION F: TOURISTS TRAVEL CHARACTERISTICS

26. Is this your first time of travelling to Ghana? 1. No [ ] 2. [ ]

27. If no, how many times……………………………………………………..

28. What is your purpose of visit to Ghana…………………………………

……………………………………………………………………………….

29. Which of the following do you make use of during your stay, tick as many as applicable

1. Hotel/restaurant/attraction/mall Wi-Fi [ ]
2. Credit card [ ]
3. Automated Teller Machine (ATM) Card [ ]

THANK YOU