INVESTIGATING SELF EFFICIENC OF CYBERCRIME ON SOCIAL MEDIA AMONG UNIVERSITY STUDENTS

A THESIS SUBMITED TO THE GRADUATE SCHOOL OF APPLIED SCIENCES
OF
NEAR EAST UNIVERSITY

By
DEMO AYELE TONKOLU

In Partial Fulfillment of the Requirements for the Degree of Master of Sciences
in
Computer Information System

NICOSIA, 2019

DEMO AYELE TONKOLU

INVESTIGATING THE SELF-EFFICIENCY OF CYBER CRIME ON SOCIAL MEDIA

NEU
2019

INVESTIGATING SELF EFFICIENCY OF CYBERCRIME ON SOCIAL MEDIA AMONG UNIVERSITY STUDENTS

A THESIS SUBMITED TO THE GRADUATE
SCHOOL OF APPLIED SCIENCES
OF
NEAR EAST UNIVERSITY

By
DEMO AYELE TONKOLU

In Partial Fulfillment of the Requirements for the
Degree of Master of Sciences
in
Computer Information System

NICOSIA, 2019

DEMO AYELE TONKOLU: INVESTIGATING SELF EFFICIENCY OF CYBERCRIME ON SOCIAL MEDIA AMONG UNIVERSITY STUDENTS

Approval of Director of Graduate School of Applied Sciences

Prof. Dr. Nadire ÇAVUŞ

We certify this thesis is satisfactory for the award of the degree of Masters of Science in Computer Information Systems

Examining committee in change:

Prof. Dr. Nadire ÇAVUŞ	Supervisor, Department of Computer Information Systems, NEU
Assist. Prof. Dr. Damla Karagözlü	Department of Computer Information Systems, NEU
Assoc. Prof. Dr**.** Hüseyin BICEN	Department of Computer Education and Instructional Technology, NEU

I Demo Ayele Tonkolu hereby declare that all the information in this document are retrieved and presented in accordance to the academic rule and conduct. I also declare that, as required by rules and conducts, I have fully cited and referenced all material and results that are not original to this work.

Name, Last name:
Signature:
Date:

ACKNOWLEDGEMENTS

I wish to explain my deepest thanks to many people who have helped me with the different aspect of my work. First and foremost I grant my sincere gratitude to my supervisor Prof. Dr. Nadire Çavuş for her appreciated the support, direction, and effort during the writing of my thesis. I thankfully acknowledge her recommendations and positive criticism at the same critical point in the course of this point.

I am also grateful to her for her patience, encouragement, and commitment to this thesis. I am intensely indebted to all Computer Information System lecturers Prof. Dr. Dogan Ibrahim, Assist. Prof. Dr. Seren Başaran, and Assist. Prof. Dr. Damla Karagözlü for their kindly help in completing my master courses because without you I were not reach this place.

In early stages of this research a gate relevant information regarding cybercrime on social media from the Near East University students, so, I wish to acknowledge all of the students who engaged for in this questioner and for their respective responses to the questions.

Lastly but not least I would like to thank my beloved family which has stand in behalf of me endlessly in completing this Master and although physically away from me the whole time have been always been near to my heart and my mind. Thank you for your loved and yours endure patience. Then I would like to thanks my friends those encouraged me in all things.

To my devoted mother…

Abstract

Today social media are being the greatest method of communication through the world by preparing people connected. Accordingly, the academic student has been used social media for exchanging information with friends, family, and relatives. However inappropriate usage social media causes cybercrime. Despite the rising usage in social media by academic students, there is no paper conducted on the self-efficiency of cybercrime on social media at Near East University. Therefore, this study purposes to investigate the self-efficiency of cybercrime on social media among the Near East University students. To do this study paper-based questionnaire was disseminated to the willingness students and the full answered 494 response was analyzed by using SPSS. The study was used *t*-test method of data analysis to understand the self-efficiency of cybercrime on social media by determining the variance between mean on age, gender and nationality of student. According to the result of the analysis indicated there is no significance in the difference between the age in all dimensions on the dependent variables. However, the significant difference in mean was founded between gender and nationality on Facebook and Twitter respectively. Relatively, the result of the study showed that the participants were confident in protecting themselves from cybercrime on social media. Finally, the output of this study will be used as input for academics, students, and researchers by integrating the social interaction and attitude of social media users.

Keywords: Cybercrime; Facebook; Instagram; Internet Technology; social media; Twitter

ÖZET

Bugün sosyal medya insanları birbirine bağlayarak dünyadaki en büyük iletişim yöntemi haline geliyor. Buna göre, akademik öğrenci, arkadaşları, ailesi ve akrabaları ile bilgi alışverişinde bulunmak için sosyal medyayı kullanmıştır. Bununla birlikte, uygunsuz kullanım sosyal medya siber suçlara neden olmaktadır. Sosyal medyada akademik öğrencilerin kullanımındaki artışa rağmen, Yakın Doğu Üniversitesi'nde siber suçun sosyal medyadaki öz-etkinliği konusunda bir makale bulunmamaktadır. Bu nedenle, bu çalışma, Yakın Doğu Üniversitesi öğrencileri arasında siber suçun sosyal medyadaki öz etkinliğini araştırmayı amaçlamaktadır. Bu çalışmayı yapmak için kağıt temelli anket istekli öğrencilere dağıtılmış ve cevaplanan 494 cevap tam SPSS kullanılarak analiz edilmiştir. Çalışmada, siber suçun sosyal medyadaki öz-verimini anlamak için, ortalama yaş, cinsiyet ve öğrencinin uyruğu arasındaki farkı belirleyerek *t*-testi veri analizi yöntemi kullanılmıştır. Belirtilen analiz sonucuna göre, bağımlı değişkenler üzerindeki tüm boyutlarda yaş arasındaki farkın önemi yoktur. Bununla birlikte, ortalamadaki anlamlı fark, sırasıyla Facebook ve Twitter da cinsiyet ve uyruk arasında bulundu. Göreceli olarak, çalışmanın sonucu katılımcıların kendilerini siber suçlardan koruma konusunda güvende olduklarını göstermiştir. Son olarak, bu çalışmanın çıktısı, sosyal medya kullanıcılarının sosyal etkileşimi ve tutumlarını bütünleştirerek akademisyenler, öğrenciler ve araştırmacılar için girdi olarak kullanılacaktır.

***Anahtar Kelimeler*:** Siber Suç; Facebook; Instagram; İnternet teknolojisi; sosyal medya;Twitter

TABLE OF CONTENTS

CHAPTER 4: RESEARCH METHODOLOGY

CHAPTER 5: RESULTS AND DISCUSSION

CHAPTER 6: CONCLUSION AND RECOMMENDATIONS

APPENDICES

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVATIONS

ASSOCHAM:	Associated Chambers of Commerce and Industry of India
ICT:	Information Communication Technology
SC:	Scale Creation
SNS:	Social Network Services
SPSS:	Statistical Package for Social Sciences
XSS:	Cross-Site Scripting

CHAPTER 1
INTRODUCTION

This is the introduction section that describe the back ground of the tittle, the problem statement, aim of the study, importance of the study, significance of the study, limitation of the study, and thesis organization.

1.1 Overview

Social media are defined as an internet-dependent application formed to promote social intercommunication and for diffusing, using and developing information through society (Kapor et al., 2017). It has the most important of our life and it's become inseparable tools in human usage by providing their effectiveness and usefulness. Social media is designed on the various concept and relays on the technology of web 2.o, ultimate essentially, the establishment and transfer of user originated content (O'Reilly, 2007). The advantage of social media was to allow a group of people or persons to exchange information with people through the use of the network. The field of computer information system is deals with the investigation of information technologies influences an individual, societal status and organization.

One of the present powerful impressions of new technology phenomena is the invention and widespread of a subclass of information telecommunication technology which referred to as social media (Kapor et al., 2017). Relational web-dependent communication tools have long been examined by information system researchers and Social media are, nevertheless, qualitatively unlike from old media and operational communication systems. Social media performs a major role at each individual and structure levels in today's modern society. With the fast-rising of information communication technologies (e.g. web and Smartphone), it's has grown up into a cornerstone tool in people's lifestyles and structure activities. Alternatively, it is difficult to define social media because of its unsteadiness since its evolution, however, it has been created for a human being to develop communication and exchange information across the world.

Social media is made up of users who interrelate with others while meeting other users through the connections established by the user list, also offering the possibility of exchanging ideas, reacting to publications and sharing Data (Morselli, 2011). Social media sites, like Facebook, Twitter, and Instagram knew and have been used for a different function. It has been demanded that users bellow twelve years old have at least more than one social media account.

The development of internet technology (IT) has completely changed everyday life. New technology like computers and social media platforms becomes a part of our life. Internet technology is defined as the system by which several computers and mobile devices around the world which interconnected through the internet which permits the interchange of data,

, knowledge, communication, and wisdom. Social media has ended up a fundamental aspect in our everyday activities; and relay at the cornerstone of the main infrastructure around the space and key elements; especially in the technology leading countries. This is rarely shocking as the fast growth of information communication technology and connectivity of the satinet in today's facts age open the door to growth productivity, speedy communication, and immeasurable convenience. Unfortunately, our extended dependence on ICT and the vast interconnectivity of our ICT facilities enforce us to include the spectrum of cybercrime threats (Sherchan et al., 2013).

The term cyberspace first produces in 1982 by William Gibson in his dumpy story burning chrome to refer to the electronic produced virtual reality. The root cyber is also concerned with cyborg; a term that defines a human system synthesis resulted from joining the human body in better high teach devices. Cyberspace defined as (Fourkas, 2018) the space in which communication among the computer networks takes place. It has produced fresh opportunities for global risk on the infrastructure of sovereign states and other critical cybercrime. The general cyber breach can also even represent a risk to worldwide peace and security; want a global framework to facilitate security.

A global framework on both cybersecurity and cybercrime framework is imperative for agree measures towards risks and hurts in cyberspace and may reduce the cybersecurity digital divide for a growing country. The strategy for common perception of cybersecurity and cybercrime are wished amongst national location at all stage of economic development.

The cybersecurity framework might also minimize risks and antagonist in cyberspace, and furnish for imperative architecture in countrywide and global solutions. Dialogues and co-existence between the state on norms and requirements in cyber out to nice to achieve a common national framework. International regulation is indispensable to make the world community able to answers to cyber-attacks and cyber-crime. To achieve for general understanding, united nation convection or declaration for cyberspace that holds solutions targeted at addressing the global challenge want to be hooked up (Roderic et al., 2014).

Social media enhance information distribution and social regression by aside to social media that more customer doesn't know. However, social media is ongoing a double-edged in addition to engaged in modifying welfare, continue, humanly sustainable and as well as to enhance committing the crime (Shabnoor and Tajinder, 2016). With the booming and constant amelioration done in Social media, it has become an addictive platform in which many people did a crime without knowing its impact on the other severs of social sites (Sheltan and Skalski, 2013). The fast expansion of social media platforms eventually with internet communication has brought a huge impact on social media users including academic students. Because of easy access to internet technology, everybody can make crimes both within the person used the internet and other people do not have involved in internet connection.

Most study on social media has indicated that using social media improves the mode in people communicate within each other's and others are shown on the contrary. As (Yeboah and Ewur, 2014) indicated social media platforms enhance the spread of cybercrime among university students. One of the problems on social media was a security problem; which is a crime committed on social media by using social media as a vector. Besides, this (Sharma and Shukla, 2016) also investigated that learner's academic enactment was adversely influenced by social media by allowing them to perform the crime.

Social media stands in the literature like Facebook, Instagram and Twitter performances a crucial role when investigating the problem on social media. Therefore, social media users want to recognize the way to protect themselves from social media cybercrime and underlying the factors that enhancing the cybercrime.

As cybercrime statics, reported in 2017 the cybercrime has been increased spontaneously for the past few years to present time (Kshetri, 2013). As the report indicated about one point five million social media users have been attacked by cybercrime yearly. Besides, many people and business characteristics act carelessly when communicating through social media and email, repeatedly exchanging facts that could bring cybersecurity attacks. So, the main of this research is to understand the student's self-efficiency in dealing with cybercrime on social media and provide a recommendation on the way people deal with social media properly.

1.2 Problem Statement

Most research conducted previously has mainly concerned about the purpose of social media among users. (Loong, 2014; Langat, 2016; Davies, 2017) investigated the social media usage rather than its impacts on the users. Therefore, due to the progression of social media usage among academic students, it is essential to investigate the self-efficiency of academic students from cybercrime. One of the missing gaps of the literature was concerning the statics of self-efficiency of users from cybercrime on specified social media in particular; Facebook, Instagram, and Twitter.

The users of social media are raising daily and are everywhere. Through the use of this technology people across the world have a connection to machines and options that are not existent in previous times. All human society has promoted its old way of conversation that expresses its existence, improvement, and company (Essien, 2015). However, with the expansion of new social media adopted and continue to live new methods of communication, especially interpersonal is change to internet-based platforms. The beginning of the internet technology and the use of information communication technology devices in any human work has enhanced humans to live without territory, the borderless scene that is called the cyber world (Sergey, 2017).

Information and communication technology (ICT) has ended up a fundamental aspect in our everyday activities; and relay at the cornerstone of the main infrastructure around the space and key elements; especially in the technology leading countries. Nevertheless, there are equitable as copious advanced opportunities to attach as there are to provide possible potential danger. This is rarely shocking as the fast growth of ICT and connectivity of the internet in today's facts age open the door to growth productivity, speedy communication ability, and immeasurable convenience. Unfortunately, our extended dependence on ICT and the vast interconnectivity of our ICT facilities enforce us to include a spectrum of cybercrime threats. Currently, cybercrime is a universal problem that affects human life in all aspects. There is not merely a medium of communication to keep in touch with old and new friends but rather have become a public forum to voice opinions and mobilize people for a global rebellion through popular social media like Facebook, LinkedIn, Instagram, and Twitter. Social media have advantages and risk simultaneously the required to caution (Langat, 2016). National Analysis Agency by its origin has elaborate that each sixth cybercrime in India is taking place by social media (Rekha, 2018*)*.

The evolution and the development of social media have brought great changes to the way users interconnect with each other. The internet and mass media explain that social media are rising at the alerting rate with a similar problem and these risks are probably to grow to catastrophic and challenging to prevent if not properly manage of social media. Cybercriminals have addressed social media as maliciously acquire and serve a large number of data it has about organizations and people (Mingle and Adams, 2015). The truth that people without difficulty believe each other on social media also raises the problem as a result criminal can effortlessly entice harmless to entrust the personal secret to them (illegal access) for malicious intentions (Ellison et al., 2017).

1.3 Aim of the Study

The main purpose of this thesis is to investigate self-efficiency of cybercrime on social media among University students.

1.3.1 Research Question

The following research question was developed in order investigate self-efficiency of cybercrime on social media (Facebook, Twitter, and Instagram).

Facebook

- Are there Significant Different in between Age across the Facebook?
- Are there Significant Different in between Gender across the Facebook?
- Are there Significant Different in between Nationality across the Facebook?

Twitter

- Are there Significant Different in between Age across the Twitter?
- Are there Significant Different in between Gender across the Twitter?
- Are there Significant Different in between Nationality across the Twitter?

Instagram

- Are there significant different in between Age across the Instagram?
- Are there Significant Different in between Gender across the Instagram?
- Are there Significant Different in between Nationality across the Instagram?

1.4 Significance of the Study

This study will important for different stakeholders as it will contribute new information for social media users. The study will help different body those have faced a problem during deals with social media site. Some of the body benefits from this thesis were explained below:

2 **Students:** This study will provide information regarding cybercrime on social media, proper use of social networks and propose the way the user keeping themselves from cybercrime. So, as academic students are the primary users of social media and as well they obtain benefits from this study.

3 **Researchers:** The result of the study will be used for the researches that want to carry a new investigation on social media-related topics.

- **Social media users**: All social media users will obtain benefits from this paper, especially, the ones who do not use social media properly.

- **Governments**: Cybercrime is the series problem for a government body. Currently, many government crises happened have caused by social media crime. Therefore, the result of this study can help the government to make a decision.

1.5 The Study Limitations

The following limitation has been identified from this study:

- This thesis was conducted during a short time; because it is good to carry out by enough time for the future.
- The questionnaires used for this study were conducted at Near East University. Therefore it's recommended to conduct on the different universities for the future to obtain more relevant information.
- The data used for this study was collected from technology-based students enrolled in Near East University. For the future, it's recommended to conduct on all departments.
- During the data collection it is difficult to obtain the exact answer from the participant which makes the result of the study less accurate.

1.6 Organization of the Thesis

This study is classified in to five main chapters as expressed below:

Chapter 1: This chapter gives a general background about the topic of the study, and the problem statement. It is also concentrated with the aim of the study, the possibility of the study, research question, the significance of the study and limitation of the study, as well as the definition of the keywords used all over the thesis.

Chapter 2: This chapter involves the literature review and theoretical framework of the topic. In this section, the related studies regarding social media were review to support the topic of study.

Chapter 3: This chapter explains the methodology of the study, which provides the approach followed to carry out this study. Besides, the flow of the procedure and materials necessary for the current study was identified and discussed in detailed.

Chapter 4: This chapter is the most important area of the study in which the result of the investigation is shortly expressed by using descriptive analysis. Here we sum up the investigation by providing results, identifying gaps and discuss the result of the analysis.

Chapter 5: This chapter is the last section of the study where the conclusion of the study is expressed. In this section, the recommendation and future work of the study is also described.

Finally, the ethical approval letter, questionnaire and similarity reports are indicated in appendices part of the document.

CHAPTER 2
RELATED WORK

In this chapter, a series of related work will covered on several correlated topics in regard to the research. The following section provides a broad overview of cybercrime on social media to support the current study.

2.1 Cybercrime on Social Media

A research by Maple et al. (2015) from University of Bedfordshire has found that social media are the most common prosecution ground for cybercrime activities. According to (Perry, 2012) there are 150 settings in Facebook that are directly related to security, and it is important to note that default Facebook security settings can increase the potential for crime and put victims at greater risk.

As Yeboah and Ewur (2014) indicated social media platforms enhance the spread of cybercrime among university students. One of the problems on social media was security problem; which is a crime committed on social media by using social media as a vector. Besides, this (Sharma and Shukla, 2016) also investigated that learner's academic enactment was adversely influenced by social media by allowing them to perform the crime.

As Senthilkumar et al. (2017) Carryout survey on cyber-crime on the students at Tamil University, on his study the questionnaire was distributed to the student for data collection. The cyber-crime among university students is studied by looking at different security problem, for instance, email phishing, malicious code, and password intensity. It has been shown that the crime on social media among the university learners in Tamil Nadu is account as 30.55% involving of 16.98% male and 13.57%female.

According to Thakur and Arjun (2018) examined the study on cyber-crime among the university student by selecting 100 sample students. From their study, they understood that student commits cyber-crime due to unawareness of cyber-crime on social media. At the interface of the investigator, their goal was to study the difference between the social media of the university, pillars of communication and information sharing.

The investigation of social media elaborate on why people use social media is a very exciting question for many researchers. The study carries out on 302 participants indicated that people have used social media for purpose of entertainment and usefulness are the major reason that people use social media (Lin and Lu, 2011), in contrast, the find out different gender have a different reason of dealing with social media. However, this study does not clarify with types of entertainment is better looking for social media members.

As Harney (2012) indicated in his study sexting is the activity of sending unambiguous messages, manly between online posts or between mobile phones. This assumption was first propagated at the beginning of the 21 era and it is expressed of texting and sex where the communication is inevitable in the extensive sense of delivering a text conceivably within the message, vulgar words, videos and obscene. It is unacceptable to recognize that different images culminating up widely posted or circulated particularly when relationships stopped. The law name these images as criminal abuse or pornography. Furthermore, writing messaging on social media use is connected to sexting attitudes and behaviors. The one who mostly sends sex-related information on social media receives information similar to what they send. Such kinds of activities have been enhanced the expansion of cybercrime on social media.

According to Purser (2014) explained social media are the most platforms for cybercrime to steal identity information. The hackers of personal information distribute web applications to the target person through social media sites to access the data directly. He also expressed the prevention method of cybercrime by increasing cybersecurity and keeping precarious information setups are necessary for each social media user and economic wellbeing. So making social media secure from cybercrime was become a pillar to the growth of modern technology as well as the security of users.

A survey carry out by Alexandros et al. (2013) indicated the majority of the cybercrime made on social media had been happened by Facebook, as it’s shown in the results. Only fewer cybercrime was take place by other social media (e.g, Twitter, Instagram, window live, Badoo). This study was done on 342 participants and most of the participants hacking their personal identity through posting the photo without permission, fake photography. The statics of study indicate that out of the total number of participants 327 participants were victims of cybercrime on social media and the rest fewer participates victims by other social media. Therefore, from this survey be concluded that social media was served as vectors to commit cybercrime.

As Singh and Jaspreet (2015) stated the easy admission to the internet, accessibility of low-priced gadget and capable internet data use permits the increase of cybercrime on social media. This easy get in to the internet promote the users felling to text and chat online. In addition to this, as showed in this investigation the raising of smart phone increase day to day, and attract the user to spend more time on social media. They also expressed that present expansion of the unsecured internet café was highly contributed for the cybercrime to be take place on social media. Therefore the result of the study stated the expansion of technology have both advantage and dis advantage.

As the study conducted by Ghari (2012) in University of Jazan indicated most of the social media evolves members manage and create their identity profile and share different data and information for the group members as well as the participants of the set spending the more time on the social media. Furthermore, different software inventors are doing on creating a modern application that helps the users on the site. Commonly, the users of the social media faced many problems by making subscribing to the service that is not authorized and program that has the virus to the users account and leading to cybercrime on social media. The study summarizes that the unnecessary trust between the users and social media lead to cybercrime.

Williams et al. (2013) emphases on social media customers with the capability to manage social media evidences streams for signs of extraordinary tension that can be scrutinized in order to distinguish deviancies from the standard (low tension /levels of interconnection). Indicators about area crime, demography, and scarcity to give a multidimensional demonstration of the terrestrial' and cyber streets. Consequently, this 'neighborhood informatics' permits a means of authorized fundamentals of civil discontent through orientation to the user produced forms of social media and their joining to other, corrected, public and marketable data.

2.1.1 Cyberbullying on social media

As Tarigan et al. (2018) carry out survey the youth are the upcoming generation that use social media in compression to other class of social media users. From the survey they understood 64% of the users of social media were youth (ages 17-22). Out of the total percentage 58% were access to online actives through the help of social network. The study classified the users to understand the social media on the cyberbullying is mostly committed. So, as output of the study indicated 70.9% of cyberbullying is happened on Facebook.

Setiawan et al. (2018) investigated the increase use of social media give different advantages to its users and on the other way have will have many drawbacks if it is not used wisely particularly among the youth who have still suspected to different impact of the consuming of social media. Absence of background related to rule resulted in youth becoming victims of social media. In addition, some fundamentals intentionally help social media to commit cybercrime prepare youth to simply target for the crime on social media.

In the study carry out by Golbeck and Klavans (2015) the extent of cybercrime on social media has bring many problem, involving the questioning ended its usefulness, which, nonetheless, has not reduced its social service. New generation has highly users of social media and therefore aware enough to reduce the cybercrime on social media. For this reason different rule was developed to reduce the problem. The main idea understood from this study was new technique and method developed to prevent the cybercrime on social media.

2.1.2 Fake Profile on Social Media

Kolade et al. (2014) conducted their study on mitigating cybercrime on social media. As understood from the study fake profile on social media was one of the problems that happened to the users of social media users. In many directions, fake profiles can help hackers to collect the necessary information from online social media sites. This study had conducted a university student to mitigate the perception users and the result indicated some of the students hacked through fake profiles. Therefore the conclusion was made as fake pictures contributed to cybercrime on social media.

2.1.3 Cyber Stacking on Social Media

As Soomro and Hussain (2019) indicated cyberstalking exclusive the cyber biosphere through using the online medium or social media, which may lead feelings of boring, abuse and passionately fretfulness to the target users. Even more, the investigation showed the financial problem come with cyberstalking victims, many average of dollar was spent every by this crime when compared with traditional stacking.

Delaney (2012) identified that social media is not only a staple in the modern person's life, but that people give access to their information without considering the consequences of sharing to a larger audience. Indeed, technological transformation does not happen within a social space and social disorder in the face of technological alteration is not new.

2.1.4 Phishing on Social Media

According to the CBS News (2016) indicated many users of the social media receive text message from the people they don't know. Actually, this message sent by the criminals that want to hack identity of the users. Pashing is the most important techniques of social engineering in which the hacker access to the email of users. As there result showed criminal have send millions of email to users through social media and access to the data of others without permission. Therefore, social engineering play a great role in the way criminal commit cybercrime on social media by sending virus to the users.

As Das et al. (2017) expressed phishing is a technique used for getting into sensitive data. The hacker creates a false account that similar to the legitimate ones and requests for their identifications and they get a problem after the users inter the identification. As he pointed the social media user's account close to 22% were phishing violence in 2014. Besides the numbers of phishing attacks increase from 18% to 63.3 million attacks during one year. Generally, the summary of this study indicated phishing increases from time to when social media is not used carefully.

2.2 Cybercrime and youth

As Oksanen and Keipi (2013) indicated in the study young people has more target to cybercrime on social media for the previous two decade. Beside, to age, financial status and other aspects involving gender and influential victimization relays with cybercrime oppression. Covered offline social media were a protective aspect alongside cybercrime persecution among females. Young cybercrime sufferers were more possible to be troubled about upcoming harassment. They displayed the implication of understanding both psychosocial danger features in offline and outlines of undefined online actions.

Marcum et al. (2016) by their study showed positively further effective policies and strategies can be recognized to teach young and people about protecting themselves while online. Young should be aware of who they are talking with online and desist from provided that any kinds of personal information to people they do not ascertain and belief. Similarly, further study of the purpose of social media sites and the incorrect actions of young's, along with their understanding of misrepresentative internet practices, will spread our awareness of the online activities and practices of adolescents. With this understanding, better safety measures and strategies can be developed to keep adolescents safe online.

CHAPTER 3
THEORETICAL FRAMEWORK

In this chapter the theories and concepts that are relevant to the topic of the research paper and that relate to the broader areas of knowledge being considered. Moreover, the theory about the classification and topology of cybercrime and the reason for cybercrime on social media was explained in detail.

3.1 Internet

The Internet has contributed people around the world with an enormous number of opportunities such as crime opportunities. Not any does the internet technology permits the individuals to connected with others dialogue with friend and family, encourage advanced personal relationship, access online resource, and establish personal networks, however, it also hand over an individual the opportunities of not to stay in the home nor not go away to meet the person by physical arena (Bossler et al., 2012). As a result, internets were changed how one person interacts, work and communicate with friend and so that it changes the lifestyle of the present person.

According to the investigation elaborated the users of the internet have increased to having relatively 657 million end-user worldwide. At the same time, the Internet has built many beneficial to everyday communication, and also raised opportunities for cybercrime (Marcum et al., 2013). Indeed, the use of Internet has developed a new perspective for unlawful activities committed by using internet services (cybercrimes) for instance as, cyber impersonation, and theft, cyberbullying, robbed and other criminal activity. The anticipation can happen in social media platforms like Facebook, Twitter, and Instagram.

3.2 Social Media

Types of social media disorganized with similar concepts such as web 2.0 and UGC. The term web 2.0 is used to define a new route in which software promoters and end-users begin to use the World Wide Web. The different study indicated that web 2.o holds on a platform in which all users endlessly renew the fillings and applications in a participatory and organized way. Secondly, UGC is considered as the sum of all methods in which users make use of social media (Kaplan and Haenlein, 2010). The combination of web 2.0 concepts and UGC with the concept of social media is delineated as follows;

A cluster of Internet-dependent applications that devolve on the ideological and technological foundations of internet two.0, which permits the preparation and exchange of User-created Content (Kaplan and Haenlein, 2010).

Social media are internet-dependent application formed to promote social intercommunication and for diffusing using and developing information through society. It is designed on the various concept and relays on the technology of web 2.o, ultimate essentially, the establishment and transfer of user originated content (O'Reilly, 2011). The use of social was to allow a person or a group of people to exchange information with each other through the use of the network. On the other hand, it is difficult to define social media because of it unsteadiness since its evolution, however it has been created for a human being to make communication and sharing information throughout the world. Social media is made up of users who interact with each other while meeting other users through the connections established by the user list, also offering the possibility of exchanging ideas, reacting to publications and sharing data (Morselli, 2011).

Most people will usually use social media, even with the exponential problem that exists, because it holds us connected. According to the national investigation agency report indicated around 70% of cyber-crime in India is caused by using of social media (Sunakshi et al., 2014). Nowadays, cybercrime is widespread in various forms such as cyber terrorism, spreading obscenity scenes, infiltration and defamation of personal privacy. (Morgan, 2014) explored the advantage of using social media in comparison to its crime committed by using different social media site like Facebook, Twitter, and Instagram. It is simply expressed as, a combination of applications that depend on the Internet, which allowed users to create and share information. Today's social media such as Face book, Instagram, and Twitter are used mostly by the youth to chat, stay in touch and meet new friends. However, as the saying goes: Not all glitter is golden, these social media have also been disadvantaged.

Social is no longer easily kinds of amusement for present younger generations. They disturb everyone, clients as well as organizations. Commercial executives, advisor, and decision creators alike all fight with understanding and decrypting how to good take advantage of the different social media applications that are taking place in the marketplace. Remarkably, this methods involves not only keeping one's online occurrence but also treats the increasing accessibility of information from social media applications (Peter's et al., 2013), such as communal or user-created content, user shapes, and conducts, as well as information, such as spatial positions.

3.2.1 Facebook

Facebook is a social media that targets to share culture, exchange data and communicate with friends. Being created by Mark Zuckerberg, this social media is used by Harvard University student for communication. Later, it is used by all the student and graduates from all college of education in America within one year. Facebook is an online social media software that allows the users to interconnect each other via private or group communication depending on varies authorization levels in social networks and connect other groups and share history within friend and other users. The percentage of information shared by Facebook students explains the present development of the customers to take the welfares of this technology. In addition, students mostly trust that Facebook can simplify and facilitate the teachers to accomplish their online parts of instructional project and group, assisting students' speech and giving direct advices (Dheleai and Tasir, 2016).

Facebook have provided the competence to send public and private messages to other customers and even take part in real-time instant messaging. Each of these features attached with the design of applications, assemblages, and enthusiastic pages create Facebook mostly popular for online socializing. This is simply the biggest social media site in the globe and one of the most broadly used and Facebook is perhaps the primary that exceeded the landmark of one billion users. Far from the capability to interconnect with relatives and friends, you can also admittance varies Facebook apps to purchase online and we can even marketplace or enhance your commercial, brand, and goods by using funded Facebook ads.

Today, Facebook is the leading social media tool for almost everybody around the world. It offers practical tools that can allow the ease of cyber-crimes, it is relatively a new Phenomenon that has been invented and creates an opportunity for people (Sharma, 2014).

However, this media open space for the user to share good and bad things online. Cyber-crime on Facebook aimed to determine how private data was accessible to another Facebook user without the user's permission. In 2012 Facebook compromised to a data transfer that had to make the telephone phone numbers and addresses of many of million customers to be exposed to unauthorized users. This had taken place due to a practical attach in their data where servers were given with additional information which was estimated to be secret when they needed to upload and download contact information of their online friends.

3.2.2 Instagram

Instagram is one just of different social media platform that occurs. It is a photo division mobile application that lets to require a photo, apply strainers to them, and allocate them on the platform itself like other social media platform Facebook and Instagram. Also, Instagram is the leading important social media prepared typically for mobile purpose. In one firm’s website, Instagram involves four hundred million active users per month with an average of three-point five billion daily views for more than 80 million pictures posted daily on the site. More than half young’s who age between 18 and 29 report victimization Instagram so, creating them the biggest constellation of Instagram users. Instagram has augmented its popularity quicker than anyone social media tools, and this is what marks Instagram so exceptional.

According Sheldon and Bryant (2016) put in their investigations the users of Instagram have low attention on purpose within other people and more on self-promotion and personal identity, besides to other intentions involving surveillance and information collecting about the others, general coolness, documentation of life occasions, which encompasses self-initiations and showing innovative such as photography skill. Besides Facebook and Twitter, Instagram is a popular social media that has about 700 million users each day. According to the Italian security services, the center has published more than 10% of the fake Instagram account. The use of these fake accounts has recently changed from subscriber purchases to a flight account. As a result, the expansion of fake accounts leads to cyber-crime on social media.

Instagram was the first social media website born mobile. Whereas supplementary social media websites use a mobile application, Instagram was produced for mobile function. This innovative application grows into a knockout instantly. Later only one month it gets a million customer. In general, Instagram is an open source app that permits users to post photo and videos (Wood, 2015). Instagram is not based on conversational, which makes it consider as social media lite. This creates it considerably more reachable compared with a dialogue-intensive platform such as Facebook or Twitter. Someone can open an account on Instagram to begin sharing the layout and monitor other individuals, luminaries, concerns, corporations, and brands. It has also two key feature that allows the user to create a beautiful image, edit photo and served as a social media platform by sharing the photo on the user timeline. Trong (2014) identified the use of Instagram as explained below:

- take a picture or a video
- change the look and impression of the media by choosing filters
- add a description
- add a hashtag
- tag people in their videos and photos
- Geotag their photos and videos,
- search and browse other people’s images and videos,
- Like, comment, or share other people’s images and videos,
- To share their content on other social media channels like Facebook, Twitter, Tumblr and other followers.

This is imaginable because Instagram permits you to spread on multiple strainers to your picture and you can simply post them to other known social media platform, such as Facebook and Twitter. Currently, it is the portion of the Facebook Empire.

3.2.3 Twitter

Twitter is produced in 2006 and has been classified as a microblogging social media, where the people interrelate in actual time depending on 140 character tweets towards their followers. People can reverse using hashtags, mentions, and replies. Even though, reports expressing degrading popularity and advantage of twitter among diminishing investment indicated no great change in the scale of internet young users who possess energetic twitter account. According to the study of 2013 indicated one-third of the active young adults those age between 18 and 29 years have Twitter users in comparison to who used in 2014 (37%) and who used in 2015 (32%). Before the Twitter gets its recent popularity, data about the number of twitter users have challenged critique over trustworthiness as Twitter miscalculates the number of users by adding accounts that have not been online for elongated phases of time (Bennett, 2011). Nevertheless, nearly Twitter unconstrained that it holds 320 million online users with one billion distinctive monthly views to the sites from surrounded tweets.

Twitter is one of the most popular social media among its counterparts, which can be an open way for the hacker to weaken the security and access user account. In 2013, Twitter announced that information and data of about 250,000 users were affected by a network-based hacker attack to access user data. This method of attack includes username, password and email address of users of the twitter. Research conducted by the research and development Corporation indicates that Twitter is very expensive compared to buying additional credit because of its lack of security. Alongside many British researchers, it appears that many false accounts opened by different users are mainly used for different types of crime. University of Southern California (USC) researchers Abokhodair et al. (2015) found that 15% of the Twitter site was not opened by an official, but was a fake account. As the international search indicates, 319 million online users on Twitter have a tow account (Davis, 2016)

3.3 Reason for Using Social Media

A social media Web site is an online public of Internet users. Old social media allows any person to connect for sharing a common feeling. It allows the users to create a webpage which enables them to share self-relevant biography, interconnected to other members and link with other members. Reputable social media like Facebook, Twitter, and Instagram have three reasons to establish community, societal, provide exclusive communication potentials and provide personalization. Social media alter the way one person communicate within other person and transform the known back and forward movement of physical to physical communication when one user must provide a route to the others while other users start interaction within other. As the investigation indicated people have been used social media for three main reasons as follows (Fisher et al., 2016):

1) Consumption of content satisfies needs for information, entertainment, and mood management.

2) Interacting with content and other users enhances social connections and virtual communities.

3) Producing own content fulfills self-expression and self-actualization.

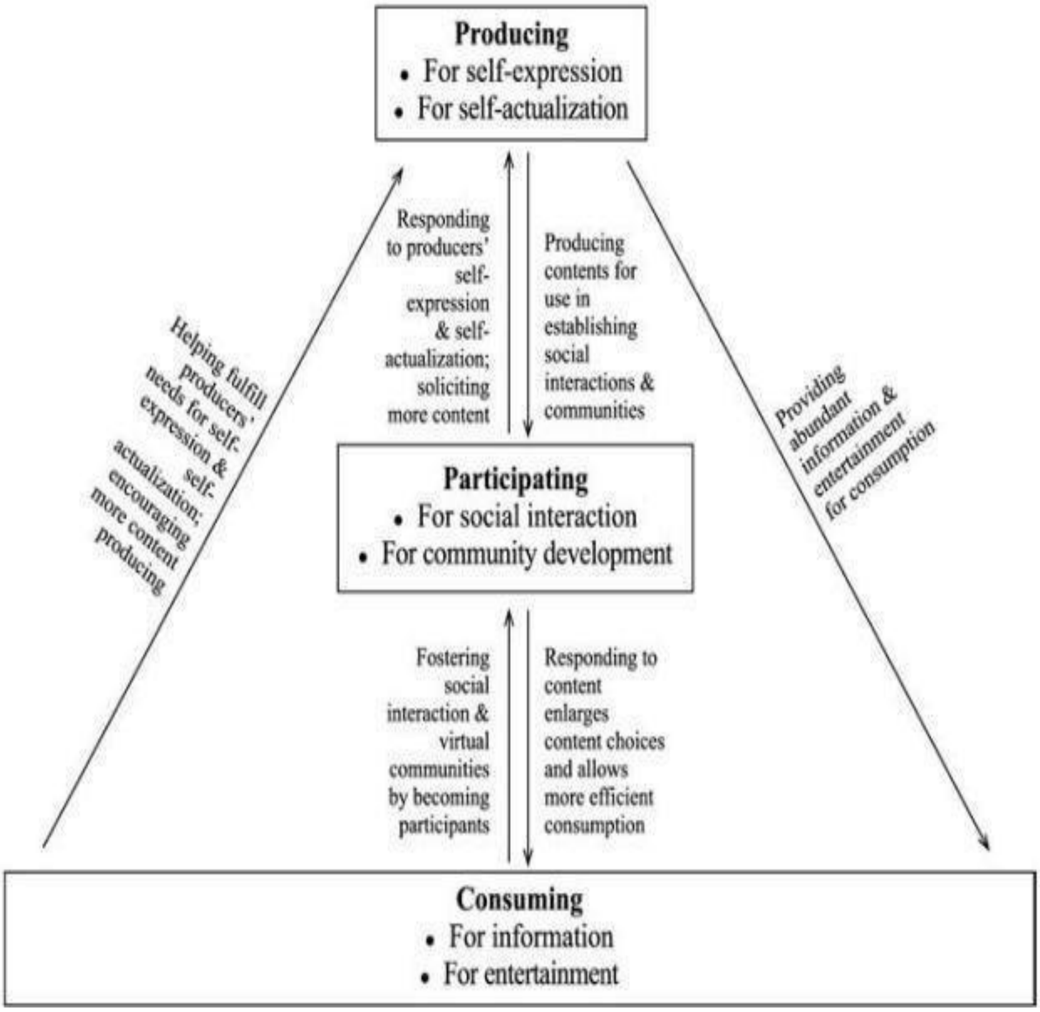

Producing
• For self-expression
• For self-actualization
Responding to producers' self-expression & self-actualization; soliciting more content
Producing contents for use in establishing social interactions & communities
Helping fulfill producers' needs for self-expression & self-actualization; encouraging more content producing
Providing abundant information & entertainment for consumption
Participating
• For social interaction
• For community development
Fostering social interaction & virtual communities by becoming participants
Responding to content enlarges content choices and allows more efficient consumption
Consuming
• For information
• For entertainment

Figure 3. 1: Reasons for Using Social media (shao and Guosong, 2012)

3.3.1 Frequency of Social Media Use

At a recent time worldwide, electronic consumers are wasting an average of one hour and fifty-eight minutes per day on social media and texting. This number has raised by over twenty minutes from 2012 to current time. The study carries out on college student indicated the students consume between 30-60 minutes on social media (Jacobsen and Forste, 2010). The time spent on social media by older people was small when compared with the time spent by young people on social media (Jelenchick et al., 2013). Therefore, a young person was considered as the most powerful user of social media as well as easy to commit the crime come through social media.

3.4 Effect of Social Media

The modern find out about mounted that greater than half of the college students determine themselves saying just an insufficient minutes when dealing with social media, update their social media accounts before performed something else, handled their yield to the fact of social media, can’t cut down on the period wasted on social media, accept boring comments from other users of social media about their use of social media and felt complicated because of the social media use. While only 22.4% of experimented college students felt addicted to social media, this investigation between university students was expressive of internet-linked habits (Sultan, 2014). In different words, the in contemporary find out about had been addicted to social media.

Most of the current investigation on the effect of social media have corroborated the discoveries of (Lin and Ahad, 2014). Other international journals have also determined the evidence indicating that dependence on social media has destructive effects. With the development of technology and social media platform, the internet, have become more and more widespread. From the most popular, Facebook, Instagram, Twitter and look to be social media platforms that a lot of people use repeatedly in their day to day lives. For the people who are regular Instagrammers, Face bookers and/or, tweeters, the different question for investigation is whether this has any effect on their self-report or self-concept. Many experiments and studies have been carried out on the different influences that risk self-report, but there has not been a broad array of revisions on social media’s result on self-report in specific.

Recently one studies have expressed that social media use is a noble indicator of body unhappiness, eating illness indications, and life gratification in young girls (Ferguson et al., 2014). On the other hand, other discoveries have explained that growth feelings of envy are importantly related to diminished feelings of life fulfillment and self-image for women who use social media and online blogs. A lot of studies have also elaborate that social media function make individuals build negative social evaluations with the person that they keep an eye on or are relative, friends on social media websites, which brings to unexpected results on self-report (Vogel et al., 2015).

3.4.1 Impact of social media on student performance

Social media platforms have a big impact on students' academic performance as the research conducted on Malaysia indicated. However, amongst the different elements used in their investigation, the usability of time and healthy addition are the most important elements that effect on the students' performance. Time management is playing an essential role in the failure and success of an individual. This indicates the one who does not spend his time on social media have succeeded in his education and on the other hand, the one that spent his time on social media has resulted in failures (Mensah and Nizam, 2016).

As Owusu and Larson (2015) expressed the social media harms the learning inclusive performance of and besides the international journal of information technology induced that there was a multifaceted incredible inter relationship between the academic performance and social media. Finally, they conclude that many users of social media have consumed their time on social media rather than academic education and this open the door for the formation of cybercrime on social media.

3.4.2 The impact of social media activity and social networks on politics, economic and Social

According to the survey made on the impact of social media on the politic shows that most of the youth participants on online political activity. However, the reality is that online and offline political activity were completely different. Youth and adults are the main online internet user society and this may cause exploitation of politics. There is two main activity of politics such as online and offline political activity. There is a big gap different online and offline political activity and the political activity of every country were dominated by an online activity because of fast to distribute the information within short time to all users through internet. Beside the activity of politics there is some good approach of politics with a good side, complains and correct the problems and also cause political instability of every country (Theocharis and Quintelier, 2016).

The social media significantly affect the economy and social life of the community. Lack of good data can affect the economy as individual, country, and as the world as well. However, the access of networks and good accessibility of can adversely affect the economy of the individual and as the country by spreading false and hate speech, harassment, porn videos and hacking and many other factors.

3.5 Social Media and Privacy Setting

In 2015 Milanovic defines the three most predominant social media as the world most important platform were: Facebook, Twitter, and Instagram. Twitter is one of the simplest and elementary social media platforms. Users of the social media can send only limited text for another user of twitter and permit only eight individual to take the photo, like and comment when the online account is public. On the other hand, Facebook allows the users to interconnect online which is called a friend on Facebook along with the strangers, colleagues, and relatives. This platform relays on exchanging pictures, opportunity, links, and thought and linking different pages of institutions and brands.

As Milonkovic declares in his study these platforms have the users of the average of 1.01 billion users every day. When arguing the title of online deception on social media, security setting is of higher importance because of the number of personal information free on the global social media platform (Liu et al., 2011). Generally, users convince their information is secret during the selected setting are not surely presented and personal information like phone number, address, picture, family information, and other supplementary information. Many users of social media do not understand and aware of the impact of revealing Personal information on the social network site. Therefore when the users are not protected them self or keep his or her secret, they became victims of cybercrime. As cybersecurity alliance, 2015 explained to prevent the cybercrime caused online the user should review their privacy setting and security issue dealing with it.

The institution declared individual should care off to how many users information they are giving with crime and understanding what information they add to the profile to reduce this issue. Also, any online social media platform gives privacy-protecting tools that help the users by changing the setting to the best way to protect them self prom unnecessary access Face book, for instance, provides two methods that help the users: This method is a basic privacy method and advanced privacy keeping method. According to Facebook help center, 2015 explain basic privacy keeping method is a method permits the users to fix who look his/her photography, who sees his/her post, how to text message for his /her, who tags his/ her and who share information on his /her timeline. On the other hand, advanced privacy setting method prevents permit users to delete post they were tagged in, accept tags before permit the fiends to see the post, preventing the users from loading unnecessary on the timeline and allow to make the same post hidden from others.

Along with Instagram, the social media grants its users to prevent a person ignore or address comments, prepare their private post or common post. The Instagram society is enthusiastic to use impressive tools that able to support the users get supportive, protected, intact, and individual account. In spite, Twitter has an option allows the users to set them from public access. One of the positive sides of twitter was ones the user make the account private, then nobody can access longer other than the accepted and approved twitter followers. As it can hypothesize, many cybercrimes are linked with security setting on social media. This thesis have concentrated on three popular social media platform namely Facebook, Instagram and Twitter, because of many numbers of daily users.

3.6 Cyber Crime Definition and Topology

3.6.1 Cybercrime definition

Cybercrime is expressed as a horrible committed contrary to a group of individual or individual by the help of new technology for instance chat room, email, internet with the crime decide of helpfully producing emotional harm, physical and mental. The purpose of computer-dependent technologies is to committing an offensive crime over cyberspace. Different kinds of cybercrimes occur such as identity theft, cyber extortion, online scam, cyberbullying, copyright infringement, and online fraud (Oluga et al., 2014). Besides, it is necessary to know that cybercrime can exist in different angle or schema for example online website, social media platform and email.

As Paternoster (2017) showed in his work cybercrime has developed into involvement for public code and has been investigated by the use of crime theories, situational factors, and individual factors. Moreover, the internet does not stand alone to give internet connection for a laptop so, it is useful to see the different device connected to the internet to deliver and acquire data like cyber threats and cellular objects .Nowadays the trends in information and communication technologies have raised the speed of personal information exchange, storage, share, and processing to remarkable level. The result of social media allows data communication on the past incomprehensible scale; provide both function and unnecessary effect for their users and among such effect of social media function are breaches social records security, that has the redundant report in the press.

In the new world, cybercrime is considered destructive. It is an act for which penalized is charged upon persuasion. A few soft of cybercriminals are noted as blockages are these persons who are virus designer. Hacker area person who discover other laptop structure for education, pranksters are humans who try to attack others. Harassment is a cyber-despotic that happens with the aid of the internet. Computer junk mails refers to unsolicited industrial classified ads dispensed online by using email, that can from time to time raise viruses and anther tools that affect the computer and the restriction of cybercrime is relay on desirable evaluation of their behavior and taking off their affects over extraordinary degrees of society (Probst et al., 2014). Therefore, cybercrime appreciation in the modern era and their consequence over society in the coming traits of cybercrimes ware expressed.

According to an ASSOCHAM demonstrated the number of cyber-crimes exists all over the world will catch a top-level to obtain money in an unauthorized way. Whilst the relationship between crime and technology is not known, the studies suggest that crime is transposed since the 1990s, gaining new directions and establishing an array of recent obstacle and aids on policing (Brown, 2015). The characteristics of online criminal activity mean the capability criminals have needed an international reach in investigating illicit intrusions into digital networks to collect information, demolish websites or perform distributed retraction of service attacks (Clough, 2015).

For many years different scholars survey obtaining the users feeling of privacy and privacy issues that take place on social media. These studies highly focused on the most known social media called Face book. Besides, the user's perception and privacy issues the studies present the way of improvement in the obvious privacy setting given by the Face book, therefore the prevention and minimization of cybercrime on should be achieved. It was obtained that users when not understand about the privacy setting and the existing setting. Finally, he concluded that users could know of the default setting and must transform this because this method helps them from becoming the victim of the security breaches (Jabee et al., 2016).

Moreover, Face book should also have care coming up the safety for keeping from occurring every security breaches. (Yisa et al., 2016) audit the purpose of social media along with the professional risks that were happening by the college students of Northcentral Nigeria. To full fill, this studies the investigation of three organizations found in North Central Nigeria was used. Interview question was used for the studies. The people took part in answering the interview question both female and male who are undergraduate students and their lie between the ages of 24 to 29. Different discovery obtained show that the benefit of online social media was done by most users for collaborating with their friends. Else users send information regarding the position on social media. It was expressed that the advantage of the social media attack same users positively although same had to professional's different risks and attacks.

All electronic objects which can combine within the internet and capable to deliver and receive information or data could be classified as a computer when considering cybercrime

(Palmiotto, 2015). Cybercrime also involves non-financial misdeed, for example creating and disseminate data that have a virus on other device or computer or releasing confidential company information over the internet. Conceivably, the most dominant type of cybercrime as identity theft; by criminals involve the internet to access personal data or file from other sources and this can take place in phishing and phrasing. The following subsidiary section of cybercrime which thesis is focusing on is briefly described as following.

The word cybercrime has been used to explain a large variety of criminal activities that are internet dependent. Cybercrime is explained by totally different people, for instance, national security authority, policeman, criminologist, technical consultant and unprofessional persons (Brown, 2015). The explanation of cybercrime is few settled once as a result of itis outlined more generally or narrowly (Purser, 2014). Merely place, the definition of cybercrime ought to not be constricting as a result of the advancement of the technology can virtually definitely be faced to an alteration of cybercrime that is why, many like to suppose of cybercrime as an ever-shifting customary of behaviors (Gillespie, 2016). Consequently, there is no constant definition of the word cybercrime, and also there is no local and global consensus on what cybercrime means. Because of the above-explained reason the universally accepted definition of cybercrime residues elusive. Below is some example of the definition of the cybercrime:

- Loader (2013) define cybercrime as an activity that area unit either misappropriate or thought of eliciting by sure groups and that will be accompanied through worldwide connected electronic device or networks.

- A criminal activity which is dedicated using a laptop and desktop that befalls above the internet (Vito and Maahs, 2015);

- All types of crime that have been happened by using a network or computer system in a network or computer system or against a network or computer system. In standard, it includes every crime able to taking place in an electronic environment (Gordon and Ford, 2016);
- It can be any cyber-relay crime happened merely through the use of information communication technology and technology-based device, whatever the devices area unit each the target for committing the crime, and the vector of cybercrime; or cyber-

enabled which area unit ancient crimes which might hyperbolic or raise in scale or increase by the use of laptop, computer network or other forms of information communication technology (Majesty, 2016);

- Refers to strategies by those computers or different electronic devices area unit accustomed to perform criminal activities and cause damage to others (Hill and Marion, 2016).

Even though nearly individuals explained cybercrime inversely, they altogether agree on the substantial role which networked computer technologies play an indefensible role in the committing of this kind of criminal activities (Wall, 2012). Different activities which is considered as cybercrime has been categorized is fallen under the umbrella of the networked system.

3.6.2 Generation of cybercrime

To address the argument of cybercrime (wall, 2007) has recognized three kinds of generations of cybercrime, all kind of generation is unique, and the intangible differences between them can express the current differences in the possibilityof the criminal occasion.

First generation of cybercrime

The first generation of cybercrime encompasses traditional crime, anywhere computers are purely a tool, and this is referred to as low-end cybercrime. In this generation of cybercrime, it can be observed the combination of computer technology, even networked technologies. Conversely, this technology paly a great role in assisting tradition criminal act and this process is continued by different means if the machinery were unconcerned. The pillar example for this generation is trafficking in human beings trafficker would use all form of discussion and information technology which are accessible, less risky and convenient.

Second generation of cybercrime

The second generation of cybercrime is the crime which is committed over the network and it is referred to as hybrid cybercrime because of that the internet has given new possibilities for traditional methods of criminal happenings to an extent global networks. This global nature wants transjuridictional processes that look complicated to achieve.

The third generation of cybercrime

The third generation of cybercrime is known as true cybercrimes because it is exclusively produced by technology. This generation of cybercrime would not occur when the internet was gone for example phishing, ransomware, and phishing (Wall, 2015). For they are the result of the internet, this cybercrime expresses each of its transformative features.

Especially, these kinds of cybercrime prepare the physical gab amid crime and its sufferers irrelevant. Cybercriminal is disruption the interrelation among space and crime being capable to do the crime and every place wherever the technology takes place and at every time and the presence of the victims is not physically necessary. As a result, online activities become a venerable to cybercriminal immediately and unexpectedly outside normal obstacle of physical gab (Yar, 2013).

5.6 Topology of cybercrime

One of the earliest authors of cybercrime (Nguyen, 2019) recognized and set forward four kinds of topology, joining both criminal behaviors and technology. Even though it was built some time ago, walls initial typology of cybercrime is broadly understood as the cornerstone when dealing with cybercrime. Walls also supposed that cybercrime should be classified as follows:

- First cybercrime topology: is called cyber trespass
- Second cybercrime topology: is called cyber deception/theft
- Third cybercrime topology: is called cyberporn and obscenity
- Forth cybercrime topology: is called cyber violence

The above classification of cybercrime is different according to the tool or target of the illegitimate activities in the way which first cybercrime topology and second cybercrime topology refer to crime confront property'; third cybercrime topology delegates crime confront mortality and forth cybercrime topology correlated to crime confront the person (Nguyen, 2019). The argument of definitions and typologies of cybercrime specifies a common piece that, heedlessly of the diverse ways of explaining or classifying cyberspace, cybercrime, give exceptional behaviors for cybercrime. These behaviors indicate encounters not lone to individuals and commerce, however also to criminal's justice systems and government throughout the globe, in trusting with and enjoying many advantages of innovative technology.

3.7 Cybercriminals

The internet house technology or online world is developing very quickly just like cybercrime. This results in the raising of different cybercrime as noted below:

3.7.1 Cyber terrorist

Refers to the combination of cyberspace and terrorism. Cyber terrorism also explained as an unlawful intervention and assaults of threats against information stored, network and computer records there in that are executed to enforce or coerce a country's government or citizens in a high degree of political or social objectives. The best example of this problem is the attacks that cause to lost life or bodily risk, revolution, or different economic degradation would be examples. Specific assault against important infrastructures and utilities could consider as acts of cyber terrorism, relay on their effect.

3.8 Cybercrime on Social Media

3.8.1 Spam

Spam is a message that involves hateful links. The spammer can deliver wide unnecessary messages extremely posting varies links on the social media account in the form of advertisement or poster by false identification and it is considered as the major violation of Facebook by Facebook help Centre. There are various kinds of spam technique-click-jacking technique in this technique of the spam the attackers used a link that advice the users to click on the link which contains another page and deliver link that targets the victim. This method permits the attackers to commit the crime onsocial media by a single click.

3.8.2 Online identity theft

Online identity theft is the major common cybercrime. It is used to access into somebody else's personality or identity unsolicited to the users for fraud or steal money. This type of cybercrime the cyber-criminal use social media to get exact users information. Cyber-criminal used a various method like malware, phishing, hacking, ransomware, fake online profiles picture to deceive someone personality or personal information of the target (Norden, 2013). The information accessed by criminals served to commit crime or fraud and used to by some illegitimate good as well as illegal activities.

3.8.3 Phishing

Social media phishing is the primary selection among the cybercriminals and they can be used in many forms of crimes such as espionage, unlawful activities and cyberbullying. Phishing is used to deceitful person for taking friend request and collect information about them from victims. Social media pulls cybercriminals for their malicious doings. Phishing is a major antagonistic on social media in which the criminals establish and controls a pseudocode website that seems a legitimate one to motivate victims to share sensitive information by sign in. in this form of cybercrime, users understand that email is real and hit on the links and the attacker access all information (Omar, 2013).

3.8.4 Stealing confidential information

Cybercriminal can steal the necessary information during the data is transfer between social media called Facebook and third party requests. Third part requests can be served to harvest sound between the users within no consent. Confirming security of monetary authorizations might be threatening since submissions are the third event. The most important example of how Identity theft worms can be distributed on Facebook is through touching on links mentioning search out what extra users are talking about you (Tow and Dell, 2010). Monitoring social media such as Facebook, Twitter and Instagram might be considerably more hard than we think as numerous of its uses are the third party. Social Media are the first device served by criminals to get their targets.

3.8.5 Cyberbullying and cyberstalking

Some of the common problem associated social media site are cyberstalking, cyberbullying, uploading unsuitable material and facing sexual marauders. The latest survey determined that 20 percent of Americans have been affected by cyberstalking. Cyberbullying is the frequent, intentional and habitually unspecified act done to upset different person via text messages by social media, a cell phone, e-mail, instantaneous messaging and chat rooms. It can be committed by a single person or a gang of people. Cyberbullying typically refers to children or youths being the targets or victims high precisely students of community or private university are the victims. Cyberbullying can happen on social media platforms such as Facebook, Twitter, Instagram, snap chat and instant message. As the study of 2008 indicate 93% of young people were online and spent many of their time on social media. There are different problem takes place when they use social media and cyberbullying is one of the major risks.

3.8.6 Cyberstalking

Cyberstalking is the combination of cyberspace and stacking wherein ended over the period when the stacker obtains the way and monitor to a victim. Cyberstalking refers to a worsened method of online annoyance directed at a particular individual that reasons significant emotional suffering and helps no legitimate function, the doing is to irritate, emotional and alarm exploitation of another person (Rahmi et al., 2019). Both online harassment and cyberstalking can be used interchangeably over varies related literature. The person who does such actions is referred to as cyber stalkers. This person does not show them to the victim's persons, instead, they follow the victim's activity to obtained necessary information and make treats. Cyberstalking is the young form of cyberbullying (Loong, 2014). Uploading unsuitable resources such as nude pictures, obscenity, videos portraying violence and posting horrible comments are unprincipled matters that are common on social media sites.

3.8.7 Online romance

Online romance is a new form of crime on social media.in this form of cybercrime, the criminals are imaginary to pledge an interrelationship through an online dating website. Social media is used as vectors for this crime by providing more information about the target victims. The criminals build false social media account to deception victim. They direct strong passions for the target and gain faith via the victim. Once obtain the trust from the user’s they will question for the gift or some money or bank delivery and fails the victims into financial loss and trouble (Shaari, 2019)

3.8.8 Malware

Malware is a malicious virus or software that can be built to collect the person’s data or information via the unrestricted entrance of social media sites (Wani, 2017). Malware problems can bring disappearance to governmental or organizational data security and has an economic impact on the growth of one’s country. As the study of 2013 indicated, the world lass of more than 1.6 billion dollar reduction happened because of malware attack. There were different problem that faced regarding privacy issues. Among them, one has happened when a hacker fused into top friends on social media like Facebook, Instagram, and Twitter by making private information observable to the hackers. Social media malware is divided into three types that are; cross-site scripting (XSS), Trojan and clickjacking.

XSS stands for cross-site scripting means virus and this virus is used against the application. This virus is produced into webpage code. Attackers or cybercriminals use XSS virus to steal, takeover social media account, and initiate users to download malware.it is distributing malicious code by using a script that permits the users to obtain wanted users information. This malicious code reproduces them self and contaminates social media consumers in two ways. Primary, the hackers add the malicious code into social media users profile, then anyone who observer that profile can easily be harmed by this virus.

The trojan is types of worm which have some unknown code, to giveaway user's penetrating data. The trojan is a very reputable malware risk on social media. This worm threats to be a useful tool for cybercriminals to stealing and fraud from the user's bank accounts and gather actionable data from the social media site (Omar, 2013). Trojan worms dispersed on social media by sending the message that seems too good things to the user. Thus message transmits targeted persons to a malicious virus and affects the user.

Clickjacking worm is other kinds of malware in social media. In this clickjacking techniques, the hacker or cyber-criminal builds a website which seems like trust website to pull social media user. User click on that link encompasses unseen link which Transmits user to an alternative page. As user click, it shows on their group's wall, and they additionally tick on that page and become make infected (Louw and Solms, 2014).

3.9 Reasons for Cyber Crime

As the cybercrime law has expressed human beings are defenseless so the legal system is needed to keeping save them. By applying this law to the cyberspace we might say that digital device is vulnerable because the rule of law is necessary required to protect and defend them against cybercrime (Patel and Dashora, 2017). Same reason for the vulnerability of computer was discussed below:

Capacity to store data in comparatively small space: Electronic device like the computer has special behavior of storing information in very little space. This makes to drive or remove information weather by virtual medium or physical makes it very easier to commit a crime.

Easy to access: The way to protect the computer from unauthorized access is very complicated. This problem is not from personal error while due to the complex technology.

by using the unknown virus-like key loggers and the logic bomb that can easily bargain advanced voice recorder, code, and retina imagery, etc. that can chump biometric systems and firewalls used to use different security system.

Complex: the computers run on operating systems and this operating system is made up of many codes that help the computer to function properly. The person who uses the computer is facing a problem in the same stage because the human mind is fellable. During this time the criminals get an advantage over the computer work and easily penetrate the computer.

Carelessness: Carelessness is very closely related to human behavior. So, if the one who uses the computer is not caring for the security of the information which working on results in cybercriminal to obtain access and control over the computer system.

Loss of evidence: Loss of evidence is a critical corporate and noticeable problem as every the information are consistently destroyed. Furthermore, the gathering of information outside the territorial amount also paralyzes this system of crime investigation.

3.10 The Impact of Cybercrime on Society

There several arguments on the definition of Cybercrime. According to European commission definitions, it is the criminals by using electronic devices networks as well as information technology systems and also against networks (Mariam et al., 2018). Now a day’s cybercrime is the significant impact on the society and individual especially those adapted to victims. However, cybercrime affects the physiological of the society and individual as well. There are several factors of the crime that regarding to the social media such as hacking including (account hacking, malware, crypto-jacking) , harassment including (revenge porn, trolling, crime hate and hate speech’s), social engineering including romance scam, phishing and the like are the main impact of cybercrime on the society (Jason and Nurse, 2018).

Cybercrime investigator faces many problems to control the crime online. There are several reasons that are making more complex to control the crime along online because it depends on the technological and it’s difficult to control easily due to day to day upgraded of new applications. Due to day to day spread of new technologies the cybercriminal increased continuously. According to Britain cyber report in 2017, in the UK about 50% crimes were recorded and also 68% of the UK business victims were attacked (Mariam et al., 2018). To enforce the law of cybercrime control and guide cybercrime investigation and intelligence are the main important factors. However, it’s difficult to fully control the criminal along with the cybercrime due to day to day enhancement and improvement of applications such as Facebook, telegrams, Whatsapp, Instagram, and many other applications. Those applications cause many impacts on social, political, and economical of the world.

CHAPTER 4
RESEARCH METHODOLOGY

This chapter gives a detailed overview of the methodology used for this study. Theresearch model used, the participant, the sample size, demographic information of participants, data collection tool, data analysis, and interpretation were highly explained in this chapter. Besides, to this the study schedule, reliability test of the questionnaire dimension and Gantt chart showed the milestone of research was also explained.

4.1 Research Model

To conduct this study the survey method was used. The survey is used to collect the information from the selected sample by their answers to questions. It is used to utilize the required data from the participants. The developed research model for the study was built on the three social media namely Facebook, Instagram, and Twitter across gender, age, and nationality of respondents. Currently, those social media were the most popular social media platform used by academics and it is important to know the way it is used by users. So, to fully understand the self-efficiency of cybercrime on social media the correlation and the difference among the dimension was computed. The data used to develop the research model was calculated from the participants through the paper-based questionnaire. Figure 4.1 below demonstrates the research model for the study.

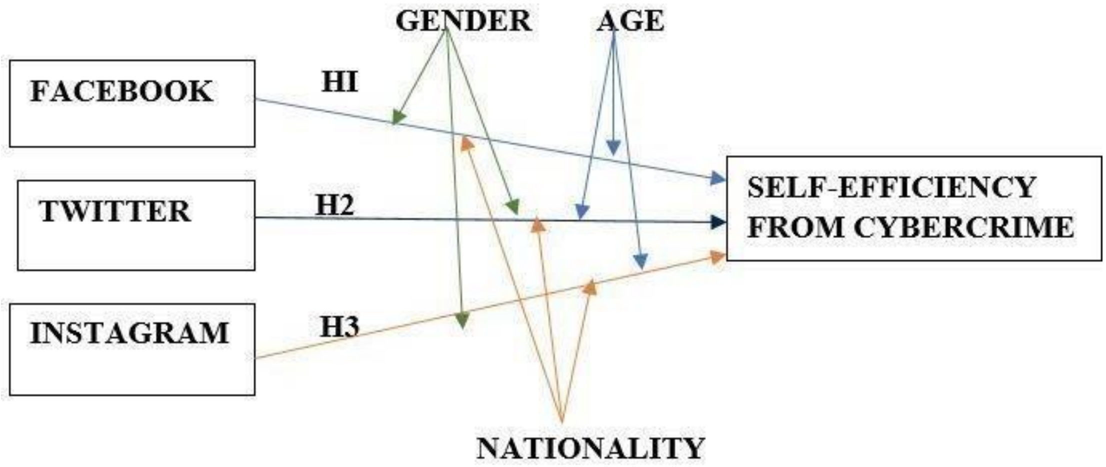


Figure 4.1: Research Model of the Study

4.2 Research Participants

The participant take an essential part in the accomplishing of this study to obtain the relevant information required for the study. The data used for the studies was gathered from the student who enrolled in a Near East University in all degree. The participant involved in the studies were selected from the technology-based students namely; Computer Information Systems, Management Information Systems, Information System Engineering, Software Engineering, Medicine, Health Sciences, Computer Engineering, and Information Technology. During the collection of the data only the volunteer's student and the users of Facebook, Instagram and Twitter were involved in the study. The survey attempted by gaining a humble random sample. Random sampling are the type of sampling helps to choose a sample of participants randomly from the selected sample without any interference. This method of sample selection allows the researchers to select the participant based on the interest of the participants. The Roan software is used to select the sample size from the total student enrolled in the school. Roan software is the machine used to estimate the numbers of the participant and it estimates 300 participants. For this study, the information collected from 494 students were used for analyses. Both primary as well as secondary data is required to conduct this study. The secondary data utilize already available information both published as well as unpublished. For primary data, however, such a facility is not available and it has to be collected by using the questionaries' method.

4.2.1 Demographic information of participants

Table 4.1 expressed participant's demographic information. As indicated in the following table the participant who participated in this investigation encompasses both male and female. 51.8% of participants were male and 48.2 % were female. This percent indicated relatively both female males were equally selected for this study. To understand the age of participants the age group is classified into three fits of rage. The first rage lay between 19- 2 2 years which have contained 19% of the total participants, the second range lay between 22-25 years and contain 33.8% of total participants and the third range were more than(>25) years and contain 47.6% of total participants. Since Near East University has different faculty the data used for this investigation were collected from different faculty of education. As seen in the next Table 4.1 5.9 % from Communication, 10.1% from Civil and

Environmental Engineering, 4% from Architecture, 21.1% from Economics and Administrative Science, 12.2% from Engineering,12.6% from Healthy Science,10.9% from Law 9.7% from Medicine, 6.1% from Pharmacy, 3.4% from Tourism and 4% from faculty of Sport Science faculty. Besides, to the above expressed information the data used for the study was collected from students come from different nationality namely; TRNC= 3.4%, TC= 5.1%, Nigeria= 29%, Ethiopia= 8%, Libya= 12%, Zimbabwe= 10.9%, Sudan= 6.7%, Jordan= 5.9%, Egypt= 9.1%, Iraq= 3.6% and 5.1% from soud Arabia.

Table 4.1: Demographic information of research participants (494 participants)

Demographic variables		**Number**	**Percentage (%)**
University	NEU	492	100
Gender	Male	256	51.8
	Female	238	48.2
Age group	19-22	94	19.0
	22-25	165	33.4
	>25	235	47.6
Faculty	Communication	29	5.9
	Civil & environmental engineering	50	10.1
	Architecture	20	4.0
	Economics and administrative science	104	21.1
	Engineering	60	12.1
	Healthy science	62	12.6
	Law	54	10.9
	Medicine	48	9.7
	Pharmacy	30	6.1
	Tourism	17	3.4
	Sport science	20	4.0
Nationality	TRNC	17	3.4
	TC	25	5.1
	Nigeria	144	29.1
	Ethiopia	40	8.1
	Libya	63	12.8
	Zimbabwe	54	10.9
	Sudan	34	6.9
	Jordan	29	5.9
	Egypt	45	9.1
	Iraq	18	3.6
	Saudi Arabia	25	5.1

4.2.2 Social media usage

Below Table 4.2 expressed the participant's social media usage. As showed in the below table 1.6 % of the respondent have been used social media for 3-4 months, 9.1 % of the total participants have been used social media for 2-5 years and 89.3 % were used social media more than (>5) years. This value indicated most of the participants selected for this study have been used social media for a long period of time. Regarding the repetition usage of social media, 98 % of the total participants were used social media every day and only 2% percent of the participants are used for a couple of months. There also result indicated the time spent on social media per day. 12.6% of participants were 0-1 hours, 24.5 % were spent 2-3 hours, and 31.2 % were spent 4-5 hours and 31.8% were spent >6 hours on social media per day. These statics indicated a high percentage of the participant spent more than six hours on social media by a day. Since the use of social media, it is important to control social media to maintain its security. In terms of controlling their social media per day 13.3 %, were control once, 13.4% controlled twice, 17.8% controlled 3 times, 24.7% controlled 4.5 times, and 17% controlled 11-15 times per a day. This percentage indicated relatively high numbers of participants were control their social media three times per day. Participants are control their social media account for different purpose. 34.6% were control their social media to update their status, 1.6 % were control their social media to specify their location, 20% were control their social media to follow what their friend are doing. 13.6 % were used social media to see where friends are at that time and 30 % of respondents select other and put their perception. As their answers indicated they control their social media to study what is new and what is going on in the social media community, check study-related news, to communicate with friends and family members and to learn education-related video have the idea of respondents.

Table 4.2: Participants social media usage

Demographic variable		**Number**	**Percentage (%)**
For how long have you been using social media?	3-6 Months	8	1.6
	2-5 Years	45	9.1
	>5 Years	441	89.3
How often do you use social media?	Every day	484	98.0
	Couple of time in a month	10	2.0
How many hours do you spend on social median in a day?	0-1 hours	62	12.6
	2-3 hours	121	24.5
	4-5 hours	154	31.2
	> 6 hours	157	31.8
Frequency of controlling social media in a day?	Once	68	13.8
	Twice	66	13.4
	3 times	88	17.8
	4-5 times	122	24.7
	6-10 times	66	13.4
	11-15 times	84	17.0
For what reason do you control your social media account?	To update my status	171	34.6
	To specify my location	8	1.6
	To follow what my friend are doing	99	20.0
	To see where my friends are at that time	67	13.6
	Other	149	30.2

4.3 Data Collection Tools

Questionnaire was used as a data collection tools in this study. Paper printed Questionnaire was distributed to the respondents directly and their answers were asked. The method and tools used for data collection were called questionnaire. The questionnaire aims to understand the student’s perception, feeling, emotion and opinions regarding the research topic. The survey used in this study has three sub-dimensions to obtain demographic information, social media usage and self-efficiency of cybercrimes on social media.

Section 1- Demographic Information: The first section of data collection tools is used to understand the biography of the participant since the participant has a different background. The demographic information section is important to decide whether the selected participants are fulfilled or not fulfill the required criteria to collect data. This part includes personal information, such as gender and position of education, Nationality, age, and faculty of education.

Section 2- Social Media Usage: This part aims to describe the social media usage habits of the participants. Five questions were asked regarding the participant's social media usage and the answer was statistically analyzed. This section described the question like ‘For how long have you been using social media?’, ‘How often do you use social media?’, ‘How many hours do you spend on social media in a day?’, ‘Frequency of controlling social media in a day?’, ‘For what reason do you control your social media account’. This question is to add extra information for the researchers to understand the social media usage by the students.

Section 3- Self Efficiency from Cybercrime on Social Media: The third section discussed the self-efficiency of participants from cybercrime on social media. The scale used for this study was developed by the researcher under the help of supervisors. This section depends on three social media platform namely; Facebook, Instagram, and Twitter. A total of 19 questions were asked regarding the self-efficiency of cybercrime on social media. Among the total questions 9 questions were asked on Facebook, 6 questions were asked on Twitter and 4 questions were asked on Instagram. Each of these variables was scaled by using a five- point Likert scale with “Not very confident (1), not confident (2), neutral (3), Confident (4), strongly confident (5). To investigate the attitudes on legal grounds, the statements “Not very confident (1), not confident of cybercrime (2), neutral (Not Sure) (3), Confident of cybercrime (4), strongly confident of cybercrime (5) have used. A total 515 paper questions were distributed to the participants and the responds of 494 were used for data analysis. The remaining 21 response was not fully answer accordingly. Finally, this section gives detailed information on the self-efficiency of cybercrime on social media Facebook, Twitter and Instagram feature among the University students. As Abdulahi et al. (2014) showed in the study social media platform like Facebook, Twitter and Instagram might use it negatively and cause damage to personals life, however, if the users of the social media read and understand the security and privacy options the might less be exposed. Khan (2012) investigated that people remain unaware of information-sharing policies, although the laws are deeply stated. This discovery also demonstrates that people do not know how their data can be shared. And they end up sharing their personal information with unauthorized people because of their ignorant attitude. Also, they noticed that the complexity of privacy settings and lack of control provided to the user is equally responsible for unintentional information sharing.

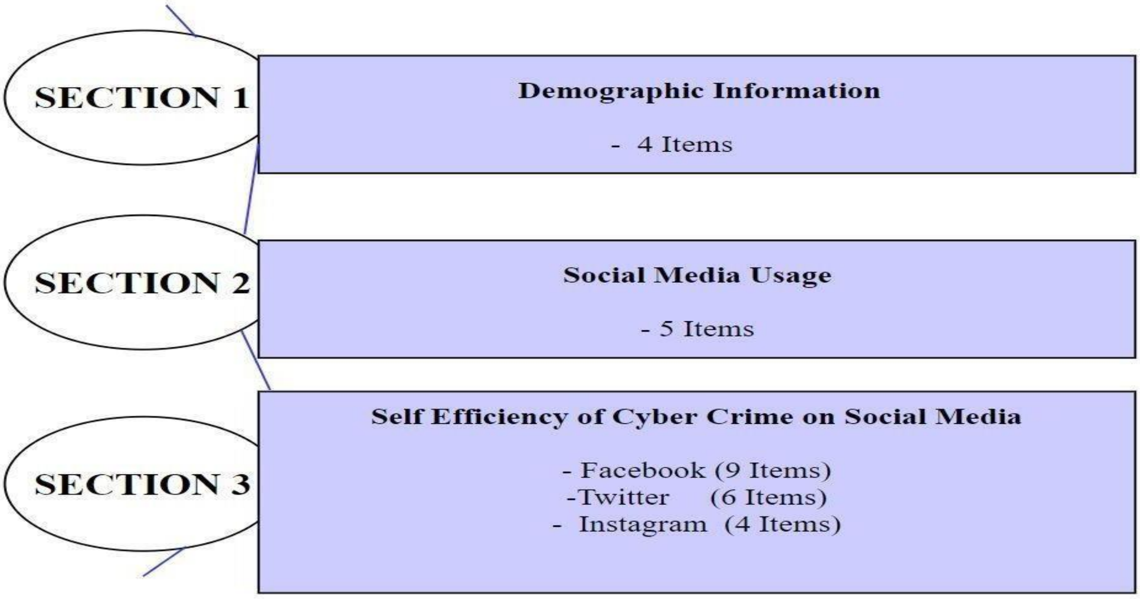


Figure 4.2: The illustration of Questionnaire Structure

4.3.1 Source and Nature of Data

Both primary and secondary data, have been collected and used for this study. Primary data is collected by using a questionnaire.

Primary data: Primary data was obtained through a survey from the participant. Such data is first hand and original. This data will be gathered from Near East University through a questionnaire.

Table 4.3: Questionnaire dimensions and Reliability test

Dimension	Numbers of Items	Cronbach's Alpha
Facebook	9	0.846
Instagram	4	0.861
Twitter	3	0.832
TOTAL	19	0.846

Method of Data Analysis

Reliability analysis is the most important part of data analysis since the consistency of the data is necessary. In reliability analysis, the consistency between each item used for analysis is calculated by using Cronbach's alpha. Cronbach's alpha is referred as a measure of reliability in data analysis and it's the highly used when you are dealing with multiple Likert scale query in the survey or questionnaire that create a scale and to find if the scale is reliable. Cronbach's alpha indicate the inter-correlation of among the item used for study. In scientific explanation, internal consistency has difference interpretation where; α is greater than or equal seven (0.7 <= α), it is acceptable and used for data analysis. A low value of Cronbach's alpha indicates the relationship between the items used in the study is poor and not acceptable for scientific analysis.

The value of correlation coefficient lie between -1 and +1. The positive value of correlation coefficient indicate the relationship between variable was strong. On the other hand the negative value of correlation coefficient indicate the negative association between the two variable. Beside this if the value of the correlation coefficient was zero, then the relationship between the variable is week. Pearson correlation (r) is the common types of correlation used for this study. It is used to measure the percentage of association between closely related variable.

4.4 Ethical Consideration

Ethics approval has been decided for this research in correspondence with the application number YDÜ/FB/2018/46 and evaluated by the Scientific Research Ethics Committee and granted approval. Ethical consideration is the process of following the rule and regulation necessary to researching by using what is right in the study. There are different ethical consideration principle that was applied and used in this investigation. These principle were; protection of participant from harm, ensuring the confidentiality of the research data and the question of deceptions of subject. Informed consent is the main ethical issue in accompanying research. It means that a participant knowingly, willingly and perceptively, and in a vibrant and evident way, provide his consent. Informed consent is one of how patients right to autonomy is protected. Therefore, this study was protected the participants from physical and physiological harm and the data collected from them do not used for other purpose. The primary ethical concerns are potential harm towards the researcher, the protection of the identities of observed individuals, and risks related to the nature of the data collected.

4.5 Research Procedure

Table 4.4 below indicate the research procedure required to accomplish this study and the duration of time required for each task. Each task in research in the thesis required appropriate time to perform the function properly. The brief description of the research procedure was described as follows:

1. The literature review was carryout first to understand what is studied on cybercrime on social media before the investigation. It helps the researcher to understand the area of the study as well as the gab of the study.

2. Thesis proposal was computed and submitted to the supervisor for review

3. The questionnaire was drafted and submitted to the supervisor and the correction was done on the questionnaire.

4. Testing of the questionnaire sample data, it is used to understand the internal consistency of the prepared data.

5. The tested sample data were analyzed and the feedback was included.

6. After the sample of data tested and feedback included the questionnaire was distributed to the participants.

7. The questionnaire distributed to the student was collected and the response of the students was feed to the SPSS software. Then the data were analyzed statistically.

8. Ones the data was analyzed by SPSS software; then chapter 4, chapter 5, and chapter 6 were compiled accordingly.

9. All document was succumbed to the advisor for review

10. The feedback of the supervisor was corrected and amended based on the comment obtained from the supervisor

11. After the comment of the supervisor was corrected; the final version of the document submitted to the Jury member and supplementary feedback were taken to concerns.

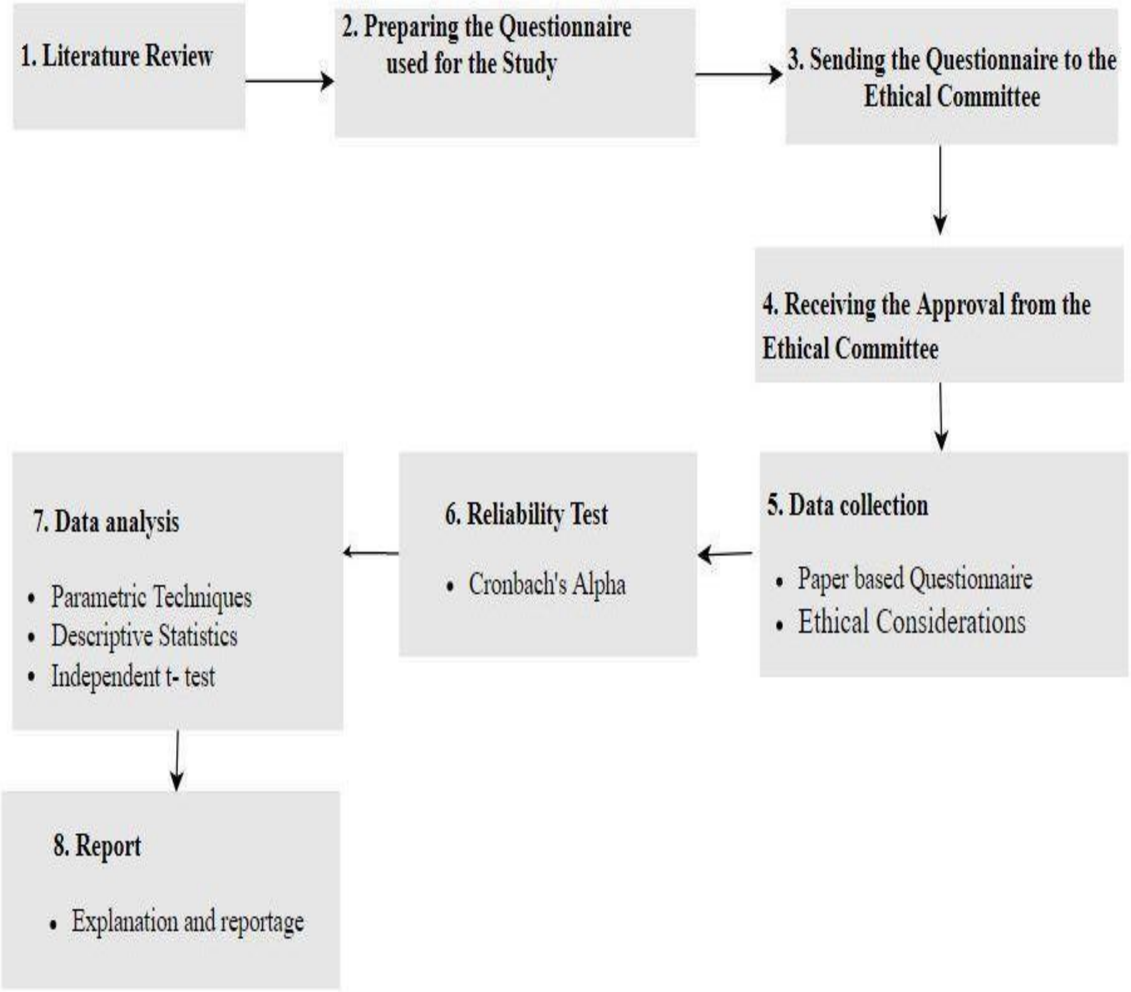

1. Literature Review
2. Preparing the Questionnaire used for the Study
3. Sending the Questionnaire to the Ethical Committee
4. Receiving the Approval from the Ethical Committee
5. Data collection
• Paper based Questionnaire
• Ethical Considerations
6. Reliability Test
• Cronbach's Alpha
7. Data analysis
• Parametric Techniques
• Descriptive Statistics
• Independent t- test
8. Report
• Explanation and reportage

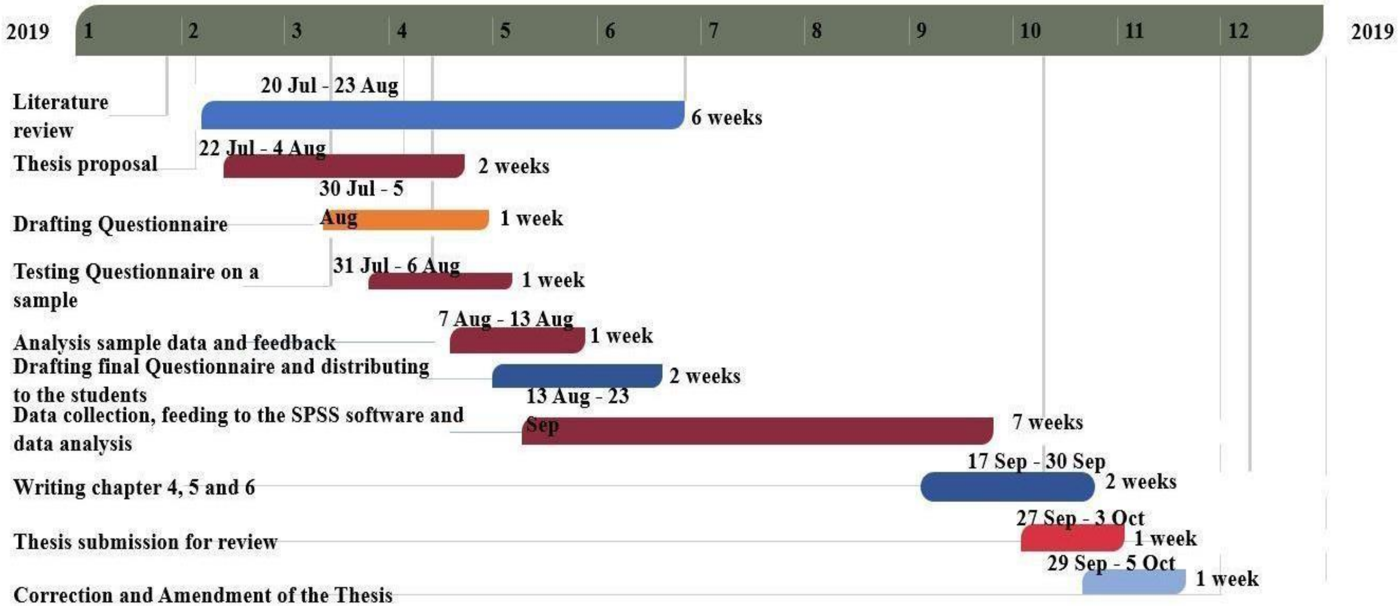
Figure 4.2: Research process and Procedure

4.6 Research Schedule

The research schedule is the most important element of research to be considered during the thesis carry out. It is the time required from starting to the final document submission. If the schedule is not fixed properly it's difficult to accomplish the task on time. So, this study has been started on since May in the year 2019 and was finished during the October year 2019. During the study was carried out the schedule is classified for each activity depending on the duration for each activity. Table 4.4 below depicts the time required for each activity in terms of weeks.

Table 4.4: Thesis research schedule

Procedure	Durations (Weeks)
Literature review	6
Thesis proposal	2
Drafting Questionnaire	1
Testing Questionnaire on a sample	1
Analysis sample data and feedback	1
Drafting final Questionnaire and distributing to the students	1
Data collection, feeding to the SPSS software and data analysis	7
Writing chapter 4, 5 and 6	2
Thesis submission for review	1
Correction and Amendment of the Thesis	1
Jury and Final corrections	1
Total	24 Weeks


2019
1
2
3
4
5
6
7
8
9
10
11
12
2019
Literature review
20 Jul - 23 Aug
6 weeks
Thesis proposal
22 Jul - 4 Aug
2 weeks
30 Jul - 5 Aug
Drafting Questionnaire
1 week
Testing Questionnaire on a sample
31 Jul - 6 Aug
1 week
7 Aug - 13 Aug
Analysis sample data and feedback
1 week
Drafting final Questionnaire and distributing to the students
2 weeks
13 Aug - 23 Sep
Data collection, feeding to the SPSS software and data analysis
7 weeks
17 Sep - 30 Sep
Writing chapter 4, 5 and 6
2 weeks
27 Sep - 3 Oct
Thesis submission for review
1 week
29 Sep - 5 Oct
Correction and Amendment of the Thesis
1 week

CHAPTER 5
RESULTS AND DISCUSSION

This section describes the main finding of the study obtained after the data analysis. From this section, all the research question raised in the previous section was answered accordingly. It is an important section of the thesis to writing conclusions and recommendations.

5.1 Correlation Matrix between Facebook, Instagram, and Twitter

A correlation matrix is used to describe the relationship between the selected items. In this section, the correction matrix for three selected factors was calculated to understand the self- efficiency of the cybercrime on social media. It indicates whether the selected items were interrelated to each other or not for writing the outcome. The following Table 5.1 described the correlation between the three dimensions.

Table 5.1: Correlation matrix of the developed questionnaire

Dimensions	**1**	**2**	**3**
Facebook	1		
Twitter	.862**	1	
Instagram	0.831**	0.43**	1

**The correlation obtained between three dimensions is significant at 0.01 and 0.05

As seen from the outcome of the analysis the positive association between the three dimensions was obtained. The positive value indicated that all the dimensions have a strong relationship with each other. The greatest correlation value obtained in this study was (correlation coefficient= 0.862) which obtained on Twitter and followed by Instagram (coefficient= 0.831). Facebook and Twitter have a strong correlation coefficient their value contributes high value for this study and next to this Facebook and Instagram have also strong relationship.so, the selected dimensions was used as a key to understanding the self-efficiency from the cybercrime on social media.

5.2 Difference in between Age across all the Dimensions

The statistical t-test is used to compute the difference between dimensions. It is an independent value used to calculate whether the difference between computed dimensions have a significant difference or not. Therefore, the independent t-test was calculated for three dimensions namely; Facebook, Instagram, and Twitter.

5.2.1 Difference in between age across Facebook

The t-test was used to determine the mean equality on Facebook which used to understand the difference across the dimensions. As written in the below Table 5.3 the p-value greater that the estimated value was obtained on Facebook. (Mean= 3.21) and (SD=1.22) for participant between 19-22 years, (Mean= 3.25) and (SD=1.09) for participant between 22- 25 years and (Mean= 3.19) and (SD=1.13) for participant more >25 years were calculated. Regarding to their mean difference (MD= -.04) were founded. Is the mean difference of the result indicated there is not difference between ages across Facebook. The p- value (p= .77) was also computed to understand the difference age across the items. P > 0.05 for Facebook is indicate the difference between Facebook and age is not statistically significant.

5.2.2 Difference in between age across Twitter

The t-test was used to compute the mean equality on Twitter which used to understand the difference across the dimensions. As written in Table 5.3 the p-value greater than the estimated value was obtained on Twitter. (Mean= 3.32) and (SD=1.08) for participants between 19-22 years, (Mean= 3.36) and (SD=1.06) for participants between 22-25 years and (Mean= 3.62) and (SD=.99) for participant more >25 years were calculated. Regarding their mean difference (MD= -.03) was founded. Is the mean difference of the result indicated there is not difference between ages across the Twitter. The p-value (p= .773, t= -.288) was also computed to understand the difference age across the items. P > 0.05 for Twitter indicates the difference between Twitter and age is not statistically significant.

5.2.3 Difference in between Age across Instagram

The t-test was used to compute the mean equality on Twitter which used to understand the difference across the dimensions. As written in Table 5.3 the p-value greater than the estimated value was obtained on Twitter. (Mean= 3.19) and (SD=1.09) for participants between 19-22 years, (Mean= 3.14) and (SD=1.14) for participants between 22-25 years and (Mean= 3.26) and (SD=1.15) for participant more >25 years were calculated. Regarding their mean difference (MD= .04) was founded. Is the mean difference of the result indicated there is not difference between ages across the Twitter. The p-value (p= .751, t= .31) was also computed to understand the difference age across the items. P > 0.05 for Twitter indicates the difference between Instagram and age is not statistically significant.

Table 5.2: Showing the difference between Age across Facebook, Twitter and Instagram

Items	Age	N	Mean	SD	Difference in Mean	P	t
Facebook	19-22	94	3.21	1.22			
	22-25	165	3.25	1.09	-.04	.77	-.96
	>25	235	3.19	1.13			
	Total	**494**	**3.16**	**1.12**			
Twitter	19-22	94	3.32	1.08			
	22-25	165	3.36	1.06	-.03	.773	-.288
	>25	235	3.62	.99			
	Total	**494**	**3.44**	**1.05**			
Instagram	19-22	94	3.19	1.09			
	22-25	165	3.14	1.14	.04603	.751	.31
	>25	235	3.26	1.15			
	Total	**494**	**3.20**	**1.12**			

**P-value is not significant at (0.05)

5.3 Difference in between Gender across all Dimensions

The following Table 5.3 indicated the difference between gender across Facebook, Instagram and Twitter.

5.3.1 Difference in between Gender across Facebook

T-test method of data analysis was computed to determine the dissimilarity between the genders of participants across the Facebook. T-test for difference in means were computed to determine the different take place on social media Facebook. The value of p<=0.05 for Facebook was obtained, therefore from this value, we conclude that there as significantly different between Facebook and gender of participants. The values of (t=-.32), mean=3.2070 for male, 3.2311= Female, (SD=1.13072) for male and (SD=1.15157) for female were obtained from the studies.

5.3.2 Difference in between Gender across Instagram

An autonomous t-test was calculated to determine the difference among the genders of participants across the Instagram. The t-tests are computed based on the second research question. The T-test for Equivalence of Means were computed to determine the different take place on social media instagram. The value of p<=0.05 for Facebook was obtained, therefore from this value, we conclude that there as significantly different between Facebook and gender of participants. The values of (t=-.32), mean=3.2109 for male, mean=3.2143 for female, (Mean difference -.00335) (SD=1.16250) for male and (SD=1.11012) for female were obtained from the studies. There is no significant difference of gender among the social media instagram.

5.3.3 Difference in between Gender across Twitter

An autonomous t-test was calculated to determine the variance between the genders of participants across the Instagram. The t-tests are computed based on the second research question. The T-test for Equivalence of Means were computed to determine the different take place on social media Twitter. The value of p<=0.05 for Twitter was obtained, therefore from this value, we conclude that there as significantly different between Facebook and gender of participants. The values of (t=2.05), mean=3.4375 for male, 3.5294= Female, (SD=1.07192) for male and (SD=1.01319) for female were obtained from the studies. In addition of this (Difference in mean= 0.124) is obtained. Generally there is a significant a significant different between gender and instagram.

Table 5.3: Showing the difference in between Gender across Facebook, Twitter and Instagram

Items	Gender	N	Mean	SD	Difference in Mean	p
Facebook	Male	256	3.2070	1.13072		
	Female	238	3.2311	1.15157	0.27	**.03***
Twitter	Male	256	3.4375	1.07192	0.124	**.00***
	Female	238	3.5294	1.01319		
Instagram	Male	256	3.2109	1.16250	-.00335	-.033
	Female	238	3.2143	1.11012		

**Level of .05 the difference in mean is significant

5.4 Difference in between Nationality across all dimensions

5.4.1 Difference in between Nationality across Facebook

An autonomous t-test was determined to understand the difference in nationality of participants across Facebook. This result is used to answer the search question namely; (H3: are there significant difference in nationality across Facebook?). As expressed in the Table 5.5 below, p>= 0.05 for Facebook was obtained. Therefore from the p-value above we conclude that there is not significant different in nationality across Facebook. In addition to this the (t=.95, MD=-.24) was computed from the result of analysis.

Table 5.4: Showing the difference between Nationalities across the Facebook

Items	Nationality	N	Mean	SD	Difference in Mean	t	p
Facebook	TRNC	17	3.2353	1.09141	-.24	.95	.33
	TC	25	3.1200	1.05357			
	Nigeria	144	3.1667	1.15268			
	Ethiopia	40	3.3250	1.18511			
	Libya	63	3.0794	1.06713			
	Zimbabwe	54	3.1111	1.07575			
	Sudan	34	3.4118	1.08670			
	Jordan	29	3.4483	1.03152			
	Egypt	45	3.3556	1.11101			
	Iraq	18	3.3333	1.13759			
	Saudi Arabia	25	3.6000	1.08012			

5.4.2 Difference in between Nationality across Twitter

An autonomous t-test was determined to understand the difference in nationality of participants across Twitter. This result is used to answer the search question namely; (H3: are there significant difference in nationality across Twitter?). As expressed in the Table 5.5 below, p<= 0.05 for Twitter was obtained. Therefore from the p-value we conclude that there difference is significant in nationality across Facebook at p=.01. In addition to this the (t=-1.4), MD=-.28) was computed from the result of analysis.

Table 5.5: Showing the difference between Nationalities across the Twitter

Items	Nationality	N	Mean	SD	Difference in Mean	t	p
Twitter	TRNC	17	3.4118	1.12132	-.28	-1.4	**.01***
	TC	25	4.0400	.45461			
	Nigeria	144	3.8542	1.00327			
	Ethiopia	40	4.0250	.99968			
	Libya	63	3.8571	.94795			
	Zimbabwe	54	3.8704	.91211			
	Sudan	34	4.0588	.54723			
	Jordan	29	4.0000	.59761			
	Egypt	45	3.7556	.90843			
	Iraq	18	3.7778	1.16597			
	Saudi arabia	25	4.0400	.45461			

*Level of 0.01 shows that the difference is significant

5.4.3 Difference in between Nationality across Instagram

An autonomous t-test was determined to understand the difference in nationality of participants across Instagram. This result is used to answer the search question namely; (H3: are there significant difference in nationality across Instagram?). As expressed in the Table5.7 below, p>= 0.05 for Instagram was obtained. Therefore from the p-value above the expected value helped as to conclude that there is not significant different in nationality across Instagram. In addition to this the (P=.57, t=-.56, MD=-.12) was computed from the result of analysis.

Table 5.6: Showing the Difference between Nationalities across the Instagram

Items	Nationality	N	Mean	SD	Difference in Mean	t	p
Instagram	TRNC	17	3.6471	.86177	-.12	-.56	.57
	TC	25	3.8800	1.20139			
	Nigeria	144	3.6806	1.06864			
	Ethiopia	40	3.6000	1.10477			
	Libya	63	3.5873	1.13073			
	Zimbabwe	54	3.7037	1.09251			
	Sudan	34	3.9118	.90009			
	Jordan	29	3.9655	1.11748			
	Egypt	45	3.7556	1.03475			
	Iraq	18	3.7778	.75190			
	Saudi Arabia	25	4.1200	.88129			

5.5 Summary of the Study

The summary of the study regarding the demographic information of participants across all dimensions was expressed in table 5.7 below**:**

Table 5.7: Summary of the finding

Hypothesis	Dependent Variable	Independent Variable	Mean Difference	P value	Remarks
H1	Facebook	Age	No	-.96	**Not supported**
	Twitter	Age	No	-.28	
	Instagram	Age	No	-.32	
H2	Facebook	Gender	Yes	**.03***	**Supported**
	Twitter	Gender	yes	**.00***	**Supported**
	Instagram	Gender	No	-.33	**Not supported**
H3	Facebook	Nationality	No	.33	**Not supported**
	Twitter	Nationality	Yes	**0.01***	**Supported**
	Instagram	Nationality	No	.57	**Not supported**

*****Level of .05 shows the different in mean is significant

CHAPTER 6

CONCLUSION AN RECOMMENDATIONS

In this section, all of the study result and recommendation was summarized based on the result obtained from the analysis. It is the most important section in which all study was indicated shortly. Finally, the limitation of the study was recommended for the future study.

6.1 Conclusion

Cybercrime can cause different kinds of harm to social media users. We survey students to understand the self-efficiency of cybercrime on social media namely Facebook, Instagram and Twitter. The prediction of the study helps the students and researches to understand cybercrime on social media and protect themselves from cybercrime on social media.

A compact of the study is expressed as follow:

- As a result, obtained from the survey indicated that it is not significant in the difference between age on Facebook, Instagram, and Twitter.
- Between the gender of the participants and two dependent variables (p= 0.03*, p= 0.00*) was obtained. This value showed that there is an observed significant difference in gender on these two social media.
- Between nationality of participants and one dependent variable (p=0.01*) was obtained. This value showed there was an observed significant difference between nationality and variable Twitter.

The maximum mean value obtained on Twitter indicated that Twitter is a good social media for the student to self-efficiency from cybercrime. This study also indicated students have less self-efficiency on Facebook in comparison to Twitter and Instagram.

6.2 Recommendations

There are a numbers of limitations to this study. From this study the following recommendation was made for future study:

- The study results showed that there is no statistical difference in age across Facebook, Twitter, and Instagram. This indicated that it has no impact on social media users regarding cybercrime. So, further study is recommended to understand the impact of age on social media.

- The data used for the study was collected only from Near East University. The future study is strongly recommended to focusing on the participants found in different University over North Cyprus.

- Qualitative study that involves in depth interviews can also be conducted to get an in depth view as to what students really understand during using social media.

REFERENCES

Abdulahi, A., Jalil, B., Lumpur, K., Samadi, M. B., and Gharleghi, B. (2014). A Study on the negative effects of social networking sites such as Facebook among Asia pacific University scholars in Malaysia. *International Journal of Business and Social Science*, *5*(10), 133–145.

Abokhodair, N., Yoo, D., and McDonald, D.W. (2015). Dissecting a social botnet: growth, content, and influence in Twitter. *In Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work and Social Computing* (pp.815-839).

Alexandro, W.M., Yahaya, N., Alamri, M.M., Aljarboa, N.A., Kamin, Y., and Saud, M. (2019). How cyberstalking and cyberbullying affect students open learning. *International Journal of Cybersecurity Intelligence, 1*, 56-74.

Bennet, H.N. (2011). Social media and the organization of collective action: using Twitter to explore the ecologies of two climate change protests. *Journal of Information Technology 14*(3), 197-215.

Bossler, M., Parse, W., and Gupta, V.K. (2014). Framework for user authenticity and access control security over cloud. *International Journal on Computer Science and Engineering, 1,* 56-74.

Brown, C. (2015). Investigating and prosecuting cybercrime: forensic dependencies and barriers to justice. *International Journal of Cyber Criminology, 9*(1), 55 -119.

Clough, J. (2015). Understanding information disclosure behaviours in Australian Facebook users. *Journal of Information Technology, 25*, 126- 136.

Das, K.A., McGivern, E., and Saykiewicz, J.N. (2017). A critical look at the impact of cybercrime on consumer internet behavior. *Journal of Marketing Theory and Practice, 10*(2), 29-37.

Davies, K., and Patel, P.P. (2017). Cybercrime in the society: problems and preventions.

Journal of Alternative Perspectives in the Social Sciences, 3(1), 240-259.

Delaney, P.M. (2012). How the smartphone, constant connectivity with the internet, and social networks act as catalysts for juror misconduct. *St. Thomas Law Review, 24*(3), 473-480.

Dheleai, A.L., Tasir, J., and Lim, S.M. (2016). Convenience or nuisance? the WhatsApp dilemma. *Procedia Social and Behavioral Sciences*, *155*, 189-196.

Ellison, N.B., Steinfield. C., and Lampe, C. (2016). The benefits of Facebook friends: exploring the relationship between college students use of online social networks and social capital. *Journal of Computer Mediated Communication*, *12*, 1143-1168.

Essien, C.F. (2014). Indigenous media and rural development: the case of oil producing communities in Akwa Ibom State, Nigeria. *Online Journal of Communication and Media Technologies, 16-31.*

Ferguson, C.J., Muñoz, M.E., Garza, A., and Galindo, M. (2014). Concurrent and prospective analyses of peer, television and social media influences on body dissatisfaction, eating disorder symptoms and life satisfaction in adolescent girls. *Journal of Youth and Adolescence*, *43*(1), 1-14.

Fisher, M., Boland, R., and Lyytinen, K. (2016). Social networking as the production and consumption of a self. *Journal of Information and Organization*, *26*(4), 131-145.

Fourkas, V. (2018). *What is cyberspace*: the cyber space and information, communication and technology. *Journal of Computer and Information Technology, 4,* 29-52.

Gillespie, A.A. (2016). Cybercrime: key issues and debates on cybercrime on social networksite. *Golden Research Thoughts*, *5*(4), 1–6.

Ghari, F. (2012). Use of social networks as an education tool. *Contemporary Educational Technology*, *2*(2), 135–150.

Golbeck, J., and Klavans, J.L. (2015). Issues and challenges of cyber security for social networking sites (Facebook). *International Journal of Computer Applications, 144(3),* 36-40.

Gordon S., and Ford, R. (2016). On the definition and classification of cybercrime. *Journal in Computer Virologyn. 2*, 13-20.

Harney, B. (2012). Sexting prevalent among high-school, study finds cybersex: advantages and disadvantages. *Journal of Humanities and Social Sciences*, *14*(3), 60-65.

Hill, J.B., and Marion, N.E. (2016). Introduction to cybercrime: *Computer Crimes, Laws,* *and Policing in the 21st Century*. California, PSI (pp. 365-675): Technology Collage.

Jabee, R., and Afshar, M. (2016). Issues and challenges of cyber security for social networking sites (Facebook). *International Journal of Computer Applications, 144(3)*, 36-40.

Jacobsen, W., and Forste, R. (2010). The wired generation: academic and social outcomes of electronic media use among university students. *Cyber Psychology, Behavior, and Social Networking, 45,* 275–280.

Jason, R.C. and Nurse, N. (2018). Cybercrime and you: how criminals attack and the human factors that they seek to exploit. *Journal of Network and Computer Application*, *86*, 24-33

Jelenchick, L.A., Eickhoff, J.C., and Moreno, M.A. (2013). Facebook depression. social networking site use and depression in older adolescents. *Journal of Adolescent Health*, *52*(1), 128-130.

Rahmi, S., and Michael, B. (2019). The Economic effects of social networks: evidence from the housing market. *SSRN Electronic Journal*, *126*(6), 22-62.

Kaplan, A.M., and Haenlein, M. (2010). Users of the world, unite. the challenges and opportunities of social Media. *Business Horizons, 53*(1), 59–68.

Kapoor, K.K., Tamilmani, K., Rana, N.P., Patil, P., Dwivedi, Y.K., and Nerur, S. (2017). Advances in social media research: past, present and future. *Information Systems Frontiers, 1-28.*

Khan, M. (2012). Users perceptions on Facebooks privacy policies. *ARPN Journal of Systems and Software, 2(*3), 119-121.

Kshetri, N. (2013). Cybercrime and cyber security issues associated with China: some economic and institutional considerations. *Electronic Commerce Research*, *13*(1), 41– 69.

Langat, A. (2016). Social media networking and its influences on interpersonal face to face oral communication at family level. *International Journal of Social Science and Humanities* Research, 212-220.

Lin, K.Y., and Lu, H.P. (2011). Why people use social networking sites: an empirical study integrating network externalities and motivation theory. *Computers in Human Behavior 27*(3), 1152-1161.

Liu, Y., Gummadi, K.P., Krishnamurthy, B., and Mislove, A. (2015). Analyzing Facebook privacy settings. *Nuclear Engineering International*, 35-38.

Loong, A. C. J. (2014). Examining the relationship between Facebook users and crime. *Cyber Psychology, Behavior, and Social Networking, 5,* 182–213.

Loader, D.M. (2013). Social network sites: definition, history, and scholarship. *Journal of Computer Mediated Communication*, *13*(1), 210-230.

Louw, C., and Solms, S.V. (2014). Information security awareness through the use of social media. *The 5th International Conference on Information and Communication Technology for the Muslim World, 42,* 15-20.

Majesty, E.N. (2016). Cybercrime and you: how criminals attack and the human factors that they seek to exploit. *The Oxford Handbook of Cyberpsychology, 23*, 662–690.

Maple, C., Short, E., and Brown, A. (2015). Predicting overt and cyber stalking perpetration by male and female college students. *Journal of Interpersonal Violence, 27,* 2183-2207.

Marcum, C.D., Higgins, G.E., and Ricketts, M.L. (2016). Potential factors of online victimization of youth: an examination of adolescent online behaviors utilizing routine activity theor*y. Deviant Behavior, 31*(5), 381-410.

Mariam, N., Jason, R.C., Nurse, H.,W., and Michael, G. (2018). Cybercrime investigators are users too! understanding the socio-technical challenges faced by law enforcement. *Journal of Social Issues, 58*(1), 49-74.

Mensah, S., and Nizam, I. (2016). The impact of social media on students academic performance a case of Malaysia Tertiary Institution. *International Journal of Education, Learning and Training, 1*(1), 14–21.

Mingle, J., and Adams, M. (2015). Evaluation of the impact brought by social networks on academic performance of higher learning students. *International Journal of Engineering and Information System, 2*(3), 14–24.

Morselli, C. (2011). Gang presence in social networking sites. *International Journal of Cyber Criminal, 5*(2), 844-877.

Nguyen, H. (2019). Cybersecurity governance framework in Vietnam : state of play, progress and future prospects. *Governance Systems for Cybersecurity / Vietnam*

Science, 86–98.

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

Oluga, A., Agana, H.C, and Inyiama, B. (2014). Cybercrime detection and control using the cyber user identification model. *International Journal of Computer Science and Information Technology and Security*, *5,* 354–368.

Omar, M., and Sad, Al. (2013). Threats and anti-threats strategies for social networking websites. *International Journal of Computer Networks and Communications, 5,* 53-61.

O'Reilly, M. (2011). The use of social networks as a communication tool between teachers and students. *The Turkish Online Journal of Educational Technology*, *16*(4), 126-144.

Owusu-Acheaw, M., and Larson, A. (2015). Use of social media and its impact on academic performance of tertiary institution students: a study of students of Koforidua Polytechnic, Ghana. *Journal of Education and Practice, 6*(6), 94-101.

Palmiotto, S. (2015). Social networking sites and privacy issues concerning youths. *Journal of Global Media, 22(6), 49* -58.

Patel, K., and Dashora, M. (2017). Crime and justice in digital society: towards a digital criminology. *International Journal for Crime, Justice and Social Democracy*, *6*(2), 17–33.

Paternoster, P. (2017). Social media impact and implications on society and students. *Journal for Media Literacy and Education, 32,* 1-17.

Peters, K., Chen, Y., Kaplan, A.M., Ognibeni, B., and Pauwels, K. (2013). Social media metrics a framework and guidelines for managing social media. *Journal of Interactive Marketing, 27*(4), 281–298.

Probst, F., Berger, K., Klier, J., and Klier, M. (2014). A review of information systems research on online social networks. *Communications of the Association for*

Information Systems, 35, 145-172.

Purser, S.D. (2013). Exploring and analyzing internet crimes and their behaviours. *Perspectives in Science, 8,* 540–542.

Rekha, M. (2018). Impact of social networking on cybercrimes. *International Journal of Multidisciplinary Research, 4*(4), 9–14.

Roderic, R., Grabosky, P., Alazab, M., and Chon, S. (2014). Organizations and cybercrime: an analysis of the nature of groups engaged in cybercrime. *International Journal of Cyber Criminology*, *8*(1), 1-20.

Senthilkumar, K., and Easwaramoorthy, S. (2017). A Survey on cyber security awareness among college students in Tamil Nadu. *Materials Science and Engineering*, *263*(4), 23-67.

Sergey, M., Smirnov N., and Erokhin,T. (2017). Cyber security concept for internet of everything. *Journal of Perspectives in Science, 8,* 540–542.

Setiawan, A.K., Singh, J., and Skalski, P. (2013). Does the use of social networking sites increase children's risk of harm? *Computers in Human Behavior, 29*, 40-50.

Shaari, A.H. (2019). Online dating romance scam in Malaysia: an analysis of online conversations between scammers and victims online-dating romance scam in Malaysi*a : Journal Computer Science, 23, 56-67.*

Shabnoor, S., and Tajinder, S. (2017). Social media its impact with positive and negative aspects. *Journal of Information Technology, 5*(2), 71 – 75.

Shao, C.V., and Guosong, L. (2012). Understanding the appeal of user-generated media: a uses and gratification perspective. *Internet Research*, *19*(1), 1 7-25.

Sharma, A., and Shukla, A.K. (2016). Impact of social messengers especially WhatsApp on youth: a sociological study. *International Journal of Advance Research and Innovative Ideas in Education*, *2*(5), 367-375.

Sheldon, V.C., and Bryant, M. (2016). Antecedents and consequences of online social networking behavior: the case of Facebook. *Journal of website promotion, 3,* 62-83.

Soomro, W., and Hussain, C. (2013). A survey of trust in social networks. *ACM Computing Surveys, 45*(4), 1-3.

Trigan, J. (2015). National security capability review. *Journal of Perspectives in Science, 8,* 540–542.

Sultan, A., and Christian, B. (2014). Impact of social media on personality development. *International Journal of Innovation and Scientific Research*, *3*(2), 111–116.

Sunakshi, M., Siddharth, S., and Avdesh, B. (2014). Inside of cybercrimes and information security. *International Journal of Information and Computation Technology, 4,* 835-840.

Thakur, V.R., and Arjun, N. (2018). Cybercrime awareness among students, school of social work. *Journal of Forensic Science and Criminal Investigation, 9*(2), 1-7.

Theocharis, Y., and Quintelier, E. (2016). Stimulating citizenship or expanding entertainment: the effect of Facebook on adolescent participation. *New Media and Society, 18*(5), 817–836.

Tow, P., and Dell, J. (2010). Understanding information disclosure behaviours in Australian Facebook users. *Journal of Information Technology*, *25*, 126- 136.

Trong, T. (2014). Challenges and solutions for marketing in a digital era. *European Management Journal*, *32*(1), 1-12.

Vito, F.G., and Maahs J. (2015). Criminology: theory, research, and policy of cybercrime for social media usage. *Journal of Information Technology*, 33–67.

Vogel, E.A., Rose, J.P., Okdie, B.M., Eckles, K., and Franz, B. (2015). Who compares and despairs? the effect of social comparison orientation on social media use and its outcomes. *Personality and Individual Differences, 86*(6), 249-256.

Wall, D.S. (2012). The devil drives a lada: the social construction of hackers as cybercriminals. *The Construction of Crime,* 4–18.

Wani, M. (2017).The impact of context collapse and privacy on social network site disclosures. *Journal of Broadcasting and Electronic Media, 56,* 451–470.

Williams, M.L., Edwards, A., Housley, W., Burnap, P., Rana, O., Avis, N., and Sloan, L. (2013). Tension monitoring and social media networks. *Policing and Society, 23(*4), 461-481.

Wood, C. (2015). How to use Instagram for business and pleasure. super effective ways to turn your Instagram followers into raving fans. *Amazon Digital Services,* 1-52.

Yar, M. (2012). The criminological landscape of new social media. *Information and Communications Technology Law*, *21*, 207-219.

Yeboah, J., and Ewur, G.D. (2014). The impact of what's App messenger usage on students performance in tertiary institutions in Ghana. *Journal of Education and practice, 5*(6), 157-164.

Yisa, O., and Soje, I. (2016). Online social networks: a survey of usage and risks experience among University students in North-Central Nigeria. *International Conference on Information and Communication Technology and Its Applications*, 129–133.

APPENDICES

APPENDIX 1

THE QUESTIONNAIRE

INVESTIGATING SELF-EFFICIENCY OF CYBERCRIME ON SOCIAL MEDIA AMONG UNIVERSITY STUDENTS

Dear student

Our questioner aims to investigate the student's self-efficiency from cybercrime on social media sites namely Facebook, Twitter and Instagram. You are expected to choose the answer that you feel closest to the results of this questionnaire. The result of this research will solely be used for the analysis in the research report and will not be provided to any other institution in any way.

Thank you in advance for taking the time to answer my questionnaire.

Demo Ayele Tonkolu (Master student)
Prof. Dr. Nadire Çavuş (Supervisor)

SECTION 1: Persona Information

1) Gender: a) male b) female

2) Nationality: A) TRNC b) TC c) other, please specify------------

3) **Age:** a) 18 b) 19 c) 20 d) 21 e) 22 f) 23 g) 24 h) 25+

3) Faculty: a) Applied Science b) Engineering c) Education d) Other, please specify-----

SECTION 2: Social Media Usage

6) For how long have you been using social media**?** A) 0-3 months b) 3-6 months c) 6-12 months d) 1-2 months e) 2-5 months f) more than 5 months

7) How often do you use social media? a) Every day b) once a week c) couple of in a week d) once a month e) couple of time in a month f) Once in a two month g) once a year h) don't use

8) How many hours do you spend on social median in a day? a) 0-1 b) 2-3 c) 4-5 d) more than 6

9) How many times do you control your social media in a day? a) Once b) twice c) 3 times d) 4-5 times e) 6-10 times f) 11-15 times

10) For what reason do you control your social media account (you can choose more than one option?) A) To update my status b) To specify my location c) to follow what my friend are doing d) to see where my friends are at that time e) Other, please specify

SECTION 3: Students perception on self-efficiency from cybercrime on social media (Please choose your answer accordingly).

Items	Very Confident	Confident	Neutral	Not Confident	Not Very Confident
CYBERCRIME ON FACEBOK					
1. I can secure my account against hackers.					
2. I can the only owner of my account.					
3. I can able to ensure that my profile is not used by another person.					
4. I can able to protect my information very well.					
5. I can avoid infiltration of a person /Affinity fraud.					
6. To be able to control and know the source of post or the link that appears on the wall of my Facebook.					
7. I can able to avoid my identification in the post, video and photos that can cause a problem for your personality.					
8. I can able to block request from people I do not know.					
9. I can able to create a secure password.					
CYBERCRIME ON TWITTER					
10. I can avoid a malware links that came on Twitter account.					
11. I can’t buy something from website that I have not verifies their source.					
12. I can secure the video and content that I post.					
13. I can avoid theft, that can theft my persona information and use it.					
14. I can create a strong and secure password to protect my content.					
15. I can use my account in safe way.					
CYBER-CRIME ON INSTAGRAM					
16. I can secure the content of my account from the followers I do not know.					
17. I can make my account private, to protect my content.					
18. I can make a difference between business account and personal account.					
19. I can able to report when I have a problem with my account.					

Please, check that you have filled all question before give me back.
Thank you for your time!!!

APPENDIX 2

APPROVED ETHICAL COMMITTEE LETTER

YAKIN DOĞU ÜNİVERSİTESİ

BİLİMSEL ARAŞTIRMALAR ETİK KURULU

11.12.2018

Dear Demo Ayele Tonkolu

Your application titled **“Investigating the Self-efficiency of Cyber-Crime on social Media”** with the application number YDÜ/FB/2018/46 has been evaluated by the Scientific Research Ethics Committee and granted approval. You can start your research on the condition that you will abide by the information provided in your application form.

Assoc. Prof. Dr. Direnç Kanol

Rapporteur of the Scientific Research Ethics Committee

Direnc Kanol

Note: If you need to provide an official letter to an institution with the signature of the Head of NEU Scientific Research Ethics Committee, please apply to the secretariat of the ethics committee by showing this document.