KHALED MABROUK AMER ADWEB SELF-EFFICACY OF UNIVERSITY STUDENTS' TOWARDS MOBILE PHONE SECURITY NEU 2016

SELF-EFFICACY OF UNIVERSITY STUDENTS' TOWARDS MOBILE PHONE SECURITY

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

By
KHALED MABROUK AMER ADWEB

In Partial Fulfillment of the Requirements for the Degree of Master of Science in Computer Information Systems

NICOSIA, 2016

SELF-EFFICACY OF UNIVERSITY STUDENTS' TOWARDS MOBILE PHONE SECURITY

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

By
KHALED MABROUK AMER ADWEB

In Partial Fulfillment of the Requirements for the Degree of Master of Science in Computer Information Systems

NICOSIA, 2016

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Name, Last name: Khaled Mabrouk Amer Adweb

Signature:

Date:

ACKNOWLEDGEMENTS

My deepest gratitude goes to Assoc. Prof. Dr. Nadire Cavus, for her constant encouragement and guidance. She has walked me through all the stages of the writing of my thesis. Without her consistent and illuminating instructions, this thesis could not have reached its present form.

This thesis is dedicated to my beloved family with unlimited thanks and heartfelt love, for they have believed in me and have sustained me throughout my life. A special feeling of gratitude to my hero, my wife Smia Khalfat who is indeed my inspiration and the woman who led me into the treasures of knowledge. I would like to thank my mother for her unlimited and unconditional love, and to my father who taught me how to be a real man before everything, and taught me that knowledge must be learned for its own sake. I would like to thank my sisters and brothers for their encouragement and constant love they gave me.

Eventually, to that long list of friends who have supported me all over the way from the early stage of my study until the last word of this thesis, thank you all for all the love and help you gave me, I couldn't be here without your existence in my life, this thesis would not have been possible.

ABSTRACT

Day by day the numbers of the students who are using their mobile phones are increasing. Hence this research is aimed to investigate self-efficacy of university students' towards mobile phone security. Research based model and questionnaire was used in the study where data are collected from 557 students which were randomly selected from two Universities from various faculties during the 2014-2015 Spring semester. In Libya the dependent variables are the 16 items in the questionnaire and the independent variables were age, gender, mobile phone usage, mobile phone security. SPSS was used to analyze the data; one-way ANOVA and Mann-Whitney U test were used to compare variables. The results showed that more students spend about 2+ hours daily on their mobile phones. Also, it was observed that more students use their mobile phones for social media purposes than other purposes. On the other hand there existed statistical significant difference between male and female students. Also, there existed statistical significant difference between all age groups. And there existed statistical significant difference between students using Android OS and other OS. And finally, there existed also statistical significant difference between students using social media and other purposes. This study will help the government, universities, parents and equally the students of Libyans to be more caution of their mobile phone it terms of security and also aid the government or universities on how to create proper awareness on mobile phone security amongst students.

Keywords: Mobile phone; mobile phone security; android; social network sites; student perceptions ; university students; mobile phone security; Libya

ÖZET

Her geçen gün cep telefonu kullanan öğrencilerin sayısı artmaktadır. Bu nedenle bu araştırmanın amacı üniversite öğrencilerinin cep telefonu güvenliği konusundaki öz-yeterliliklerini araştırmaktır. 2014-2015 Bahar döneminde iki üniversitenin çeşitli fakültelerinden rastgele olarak seçilen 557 öğrenciden veriler toplanmıştır. Çalışmada araştırma temelli model ve bir anket kullanılmıştır. Araştırmadaki bağımlı değişken anketteki 16 maddedir. Bağımsız değişkenler ise yaş, cinsiyet, cep telefonu kullanımı ve cep telefonu güvenliğidir. Veri analizi için SPSS kullanılmıştır; değişkenlerin karşılaştırılmasında tek yönlü ANOVA ve bağımsız Mann-Whitney U-testi kullanılmıştır. Sonuçlar daha çoğu öğrencinin günde 2 ve üzeri saatini cep telefonlarıyla uğraşarak geçirdiğini göstermektedir. Buna ek olarak, daha çok öğrencinin cep telefonlarını diğer sebeplerden çok sosyal medya amaçlı kullandığı gözlemlenmiştir. Diğer yandan erkek ve kız öğrenciler arasında istatistiksel olarak anlamlı fark bulunmuştur. Ayrıca, tüm yaş grupları arasında anlamlı farklılıklar görülmüştür. Android işletim sistemi ve diğer işletim sistemi kullanan öğrenciler arasında istatistiksel olarak anlamlı fark gözlemlenmiştir. Son olarak sosyal medya ve diğer amaçlar için cep telefonu kullanan öğrenciler arasında istatistiksel olarak anlamlı fark bulunmuştur. Bu çalışma devletin, üniversitelerin, ebeveynlerin ve ayni zamanda Libyalı öğrencilerin güvenlik açısından cep telefonlarıyla ilgili daha dikkatli olmasını sağlayacak ve devlete veya üniversitelere cep telefonu güvenliği konusunda doğru bir farkındalık yaratmaları için yardım edecektir.

Anahtar Kelimeler: Cep telefonu; cep telefonu güvenliği; android; sosyal ağ siteleri; öğrenci algıları; üniversite öğrencileri; cep telefonu güvenliği; Libya

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATION

ANNOVA:	Analysis of Variance
SMS:	Short Message Service
PDA:	Personal Digital Assistant
PIN:	Personal Identification Number
ARM:	Architictuter For the digital Module
GSM:	Global System for Mobile Communications
MMS:	Multimedia Messaging Service
UMTS:	Universal Mobile Telecommunication System
PC:	Personal Computer
OS:	Operating System
GPS:	Global Positioning System
SD:	Standard Deviation
M:	Mean
TAN :	Transactions Authentication Number
UK	United kingdom
UAE	United Arab Emirates
USA	United states of America
CIA	Central Intelligence Agency
ID	Identity
SIM	Subscriber Identification Module

CHAPTER 1
INTRODUCTION

The most ubiquitous, dynamic and refined patterns in communication are cell phones (smartphones). The cellphone is a cellular phone, making a complete working framework in such a way like a standard PC that offers moved figuring abilities and system decisions (Alfawareh and Jusoh, 2014). All activities which can be performed on PCs for instance; information sharing, getting messages and sending, visiting, opening and modifying records, paying for things, perusing and shopping should be possible using a cell phone. Some cell phones have applications of present day, for instance, a camera which can function as a scanner (Jones and Heinrichs, 2012). These parts enable new sorts of versatile administrations that in this manner shape the utilization of affinities for cell phone customers. Cell phones were released in the year 2000. The first model was R380, which was made by Ericsson. Truth be told, it was the first successful type of contraption, a converging between a mobile phone and PC helpfulness, was known as a cell phone. With the help of cellular customers, a cell phone has transformed into an especially appealing device. Nowadays, cell phones have been used to supplant desktop or versatile PCs (Alfawareh and Jusoh, 2014). As smartphones give more applications to an undeniably a more extensive scope of utilization circumstances, they have turned into an inexorably incorporated a portion of individuals' consistent life. Cell phone has been gotten by cellular customers in various countries all over the world. As indicated by Google's study in 2011, UK, Norway, UAE, Australia, and Saudi Arabia all boast cell phone choice rates above half. The reputation of cell phone is to a great degree promising. It was shown by research in 2011 that, about eighty three percent of USA grownups possess a cellular phone or something to that impact, and that 42% of them had a cell phone. That disentangles into 35% of all grown-up (Rao, 2012).

Cellphone devices are turning into a basic segment of the advanced economy, a style articulation and helpful communication gadget, an imperative piece of day by day life for billions of individuals around the globe (Androulidakis and Kandus, 2011). Utilized for individual amusement or purposes of trade, the cell phone has added to the developing energy of the remote upheaval and the m-trade blast. Cutting edge cellphones improved abilities permit them to be very nearly as flexible as a PC turning into an important business (cellphone

applications, m-trade) and diversion instrument (cellphone amusements). In the meantime clients store and handle more information incorporating delicate data in their telephones such as their credit/debit card numbers, photographs of their private life and PINs (Jones and Heinrichs, 2012).

The development of cellphone internet figuring has been not precisely stunning. By 2015 the cellphone internet is depended upon to be more prominent than the internet of desktop (Meeker et al., 2010). It was shown that by Gartner guage that cellphone of over 6.5 billion affiliations are regular by the year 2014, and individuals of over 3 billion around the globe will partake in online shopping and banking (Whitney, 2010). Telephones are giving keeping in mind the end goal to engage this advancement a secured exchanges vehicle and wallet supplanting as a store for unwavering quality e-tickets, train passes, cards, and other routine things (Kavur, 2010). The advancement of cellphone Internet figuring passes on with it rising anxiety over cellphone contraption dangers and security issues. The outcomes of Cellphone gadgets was seen and controlled by the American Institute of Certified Public accountants (AICPA, 2011) as the major advancement on its development in 2011 list took after by data security. The rundown joins movements that IT manager ought to consider all through the going with 12-year and a half. Gregg (2010) reported the making number of PDAs and other cellphone gadgets that association with the Internet as the most noticeably ghastly structure's security hazard in the year 2010. GTISC (2010) saw the dangers to VoIP and cellphone contraptions as one of the major five hazards to data security GTISC from issues, for case, malicious software, listening in, lost or stolen gadgets and phishing. Jones and Heinrichs (2012) see the true blue cellphone security issues as guaranteeing the data that sits on the contraption for those unpreventable occasions when it is left in the rearward sitting strategy of a taxi, protecting business applications from toxic change, and diminishing the cost of extending the base to consolidate these telephones.

Cellphone movements can change guideline, in the classroom and remotely, by giving surprising access to instructive assets at whatever point, wherever. Institutional plentifulness will be updated by valuable access to organizations and information from a client's gadget of decision. Correspondence among every last institutional assistant will without a doubt be

updated by flexible and energized applications truly in the palm of a client's hand. With the potential effect of cellphone contraptions on grounds, relationship of forefront direction in addition stress over security repercussions. Ingerman et al. (2011) refered to that EDUCAUSE kept arranging security if all else fails as one of the top IT issues as foundations persuade the chance to be both customers and suppliers of cloud organizations accomplishing a should think about the relative non participation of security on the gadgets that are utilized to get to our institutional assets. PDAs are one kind of cellphone contraption that can be used to start to ground assets. They are consistent on school grounds and can be utilized to start to institutional information over a system. Much the same as tablets, telephones can be enough traded off and ought to be settled to protect both the soul and the foundation (Jones and Heinrichs, 2012) Verifiably, understudies have not generally given sufficient thought concerning securing their figuring assets and can put grounds data assets at threat.

1.1 Problem of the Study

As remote communication has been quickly exceptional, cellphone applications and administrations are turning out to be more mainstream, similar to texting, downloading of an assortment of substance, cellphone trade, cellphone keeping money, and data leaks. Innovation propels has rearranged business, advanced stimulation and made individual exchanges more helpful for cellphone gadget clients, be that as it may, it has additionally opened the way to a considerable measure of security dangers. Cellphone gadgets, for example, cellphone, Personal Digital Assistant (PDA) and advanced cellphone are presented to various security dangers like malignant code (counting virus, worm and Trojan stallions), vulnerabilities of cellphone, assaults on communication, information theft and harm and cellphone spam (Kim and Leem, 2010). Besides, with an expanding measure of data being sent through remote channels, new dangers are coming up. At some point or another, data security will turn into a basic issue to cellphone gadgets and be of incredible worry to cellphone gadgets clients, much the same as what users of computer do today (Ying et al., 2010). It has been understood that data security is not only an innovation issue, and as of late it turns into a hotly debated issue to study human components in data security in the field of the internet (Jones and Heinrichs, 2012).

1.2 Mobile Phone Utilization Risks

The danger of using cellphone includes the following:

- Being assaulted by infection originating from SMS\Bluetooth\PC. For instance, Security seller SimWorks International as of late set the principal Symbian infection equipped for spreading by means of MMS messages. In addition, continuous record interpretation utilizing Bluetooth between cellphone gadgets and PC have brought high conceivable outcomes of vindictive code occurrences, which will acquire information burglary or gadget harm (Kim and Leem, 2010).

- Receiving spam messages. Spam messages for promoting or misrepresentation is thought to be an unsettling influence of clients' typical life and Spam messages might likewise carry infection with them.

- Data misfortune because of robbery or loss of cellphone gadgets. Private documents, contact data or business data will be lost with the loss of cellphone gadgets.

- Be listened in, or got to by unapproved clients. A few clients store individual documents, business contact or even classified data like charge card number in cellphone gadgets. Some of the time individuals uncover the touchy data on cellphone correspondence. The entrance of unapproved persons to this sort of data will bring about substantial misfortune (Ying et al., 2010).

- Internet trick or infection disease while getting to the system by cellphone. Different administrations, for example, web seek, email and File interpretation gave by cellphone cell processing gadgets in a remote correspondence environment have conveyed new hazard worry to others. (Ying et al., 2010).

Smith (2011) opined that Pew study reported 83% of USA adults guaranteed some kind of cellphone and 35% had a cell phone (Smith, 2011). Cell phones grant customers to store information, send and get email, present projects, and make telephone calls all in one contraption (Jones and Heinrichs, 2012). Cell phones fuse cellphone limits with the more

ordinary segments of a handheld PC or PDA. Cell phone proprietors taking an enthusiasm for the Pew (Smith, 2011) study reported utilizing a wide collection of livelihoods: Fully nine in ten mobile phone proprietors utilize content, lighting up or convey pictures with their phones, while eight in ten utilize their phone to go online or send photographs or recordings to others. Different exercises, for occurrence, downloading applications, watching recordings, getting the chance to long range interpersonal correspondence destinations or posting mixed media content online are totally restricted to the wireless individuals (Smith, 2011). PDAs are powerless against different sorts of dangers. Not these require imaginative ability.

Consider the potential harm from basically losing a cell phone. The consequences of a missing gadget were underscored by the April 19, 2010, Computer world element: Gizmodo paid $5K for bleeding edge iPhone (Keizer, 2010). The story revealed that an Apple laborer lost a cutting edge iPhone, which was later sold to Gizmodo, an online gadget guide. The vast majority losing a cell phone don't need to push over the all-inclusive community disgrace of their names appearing on a surely understood site. In any case, anyone can lose a cellphone and experience the evil impacts of revealing a plenitude of unprotected data, for instance, Visa pin numbers, account numbers, and customer messages. Panko (2010) recognizes four general sorts of security threats: Malware (infections and worms), strikes on individuals (e.g. spam, coercion, phishing, wholesale misrepresentation, and charge card theft), hacking (softening up), and repudiation of-organization (using bots). Not in the slightest degree such as leaving a phone in the back of a taxi, the risks recognized by Panko are executed with the aide of information advancement. The starting three risks are the most critical to mobile phones; foreswearing of-organization is more consistently used to meddle with an Internet site or organization. Malignant software is frequently given outcast applications. Malignant software gets to a contraption with the deciding objective of taking data, hurting the device, or chafing the customer, et cetera. (Felt et al., 2011). Trojan horse, which veils themselves as good fashioned activities, is fabulous instances of malware that can be a minor inconvenience or make honest to goodness hurt. For example, the Bootton.E Trojan horse restarted the cellphone contraption besides debased parts that made a reboot to miss the mark, leaving the device unusable. Another malware program, the Pbstealer.D Trojan, sent a customer's contact list, scratch cushion, and timetable calendar to other near to customers by method for

Bluetooth (Gohring, 2012). Ambushes on individuals, for instance, phishing, the usage of bona fide looking email or locales to ask for sensitive information can in like manner be introduced through outcast applications. For example, customers debased by one Trojan were asked for that enters their cellphone number and cell phone model for a confirmation redesign. By tapping on an association with the redesign, a threatening record was presented and drawing nearer SMS messages were abhorrence to a predefined mobile phone number (Maslennikov, 2011). Hacking, the unapproved use of a PC resource, can be executed in a couple courses with PDAs. Starting, a contraption can be adequately exchanged off if it has no approval security, for instance, a mystery word. Second, mobile phones can serve as minute issue territories that allow access to network resources. Tricks can set up fake Wi-Fi ways to which the latest time of cellphones will actually interface. Once an affiliation is developed, all the information experiencing the entry can either be scrutinized particularly or decoded using programming that will continue running on a cellular workstation (Arthur and Beggan, 2011). Strategies for lessening frameworks peril fall into four specific steps as delineated by the Security Action Cycle: Deterrence, foresight, distinguishing proof, and recovery (Jones and Heinrichs, 2012).Discouragement incorporates procedures, for example, approaches and rules that are latent in nature and rely on upon the eagerness of clients to consent. The following step, aversion, includes activities that authorize arrangement and frustrate illegitimate use. In the event that assailants do figure out how to rupture a system, recognition measures accumulate data about episodes and recognize interlopers. In the event that an interruption occurs, recuperation activities concentrate on curing the damages brought on by the misuse, for instance rebuffing the culprits. Prevention and recuperation have been portrayed as hierarchical activities comprising of non-specialized procedures. Aversion and location are frequently tended to through the reception of particular advances by people (Shropshire et al., 2010). In the realm of cell phones, advances regularly suggested for avoidance and/or recognition of misuse incorporate passwords, encryption, hostile to malware, and programming redesigns. As indicated by Clarke, the previous digital security boss for the White House, cell phones represent the most up to date and biggest powerlessness in corporate America now (Ingerman et al., 2011: 16). They are common on school grounds and can be utilized to get to institutional information over a system. Cellphone advances can possibly change direction, in the schoolroom and remotely, by giving remarkable connection to

informational resources at whatever time, wherever((Ingerman et al., 2011). On the other hand, much the same as PCs and tablets, phones can be easily exchanged off and should be secured to guarantee both the individual and the establishment. A couple thinks about have broke down the PC security practices of understudies. Teer et al. (2010) examined PC security practices of undergrads and their perspective of the essentialness of such practices. Lomo-David and Shannon (2010) examined understudies as for the relationship amidst acknowledgment and usage of 10 securities rehearses, as an illustration, clear firewalls and passwords. At of six of the ten characteristics, shared characteristic deciphered into convenient utilize; the four regions where a colossal relationship did not exist in the middle of recognition and practice were passwords of email connections, biometric confirmation, interruption identification systems, and multifaceted verification systems. With regard to the matter, Mensch and Wilkie (2011) reported an alarming separate among data security mentalities, practices, and apparatus utilization among students. The scientists underscored the requirement for an outlook change in ceaseless secure conduct.

1.3 The Aim of the Study

The primary purpose of the work is to look into the self-efficacy of University students towards mobile phone protection. To achieve this main purpose, we demand to achieve more sub aims like:

1. What is the university students' self-efficacy towards cellphone'security?
2. Is there any gender based difference on university students' self-efficacy towards mobile phones security?
3. Is there any age based difference on university students' self-efficacy towards mobile phones security?
4. Is there any cellphone operating system based difference on university students' self-efficacy towards mobile phones security?
5. Is there any cellphone phone usage based difference on university students' self-efficacy towards mobile phones security?

1.4 The Significance of the Study

The previous couple of years the primary headache of a cellphone client would be protection of his/her communication and this is not the case any longer (Audrolidakis and Kandus, 2011). Students must be shielded from unapproved outsider access to their data. It is intelligent that apart from the customary attempts to prove safety, for example, PIN usage and voice encryption, students need to consider additional efforts to make safety and strike after new best practices. Hence this work is to look into self-efficacy of University students towards mbile phone security.

1.5 Limitations of the Study

The limitations of the study:

i. This study was only limited for university students, as it was applied in Tripoli University and in Misurata University.
ii. Due to the large data required, two universities were used for this study.
iii. Time of the study was a major limitation in the sense that if this study will be carried out again at the future, the perceptions of the students will be changed towards cellphones'security.

1.6 Overview of the Study

Chapter 1 gives details about the general introduction of cellphone usage and security, the problem definition, the significance of the study, the aim of study, the limitation of this study and most importantly the breakdown of this study.

Chapter 2 presents the related research work on cellphone security, cellphone self-efficacy, cellphone usage, Gender based cellphone phone usage and Age based cellphone phone usage.

Chapter 3 introduces the theoretical system whereby various aspects of cellphone device usage and security, security considerations, cellphone operating systems and cellphone phone malicious software were discussed.

Chapter 4 gives an overview about the research methodology, in which the research model, the participants, the data collection process and the instrumentation used in the research, data analysis techniques employed, and the data collection procedure were discussed.

Chapter 5 is the section where the results and discussion were discussed in details.

Chapter 6 mentions the conclusion of the entire research study and recommendations of the thesis, suggestions, and for future studies.

CHAPTER 2
RELATED RESEARCH

2.1 Self-Efficacy on Mobile Phone Usage

A survey study made by Mobile Planet (2014) to understand Saudi Arabia mobile user, shows that respondents were requested a collection from request around device use, portable chase, video, social, web and business conduct and versatile publicizing. Regardless of the way that Google had endeavored to make a reassessment on 500 online cell phone customers, yet the investigation is exceptionally wide without focusing on a specific specialty. Examinations of examples in cell phone use among purchasers, especially students that have been led in various nations. Various areas have indicated particular study comes to fruition and finding (Alfawareh and Jusoh, 2014).

Research reports (Park and Lee, 2012; Kim and Altmann, 2013; Payne et al., 2012; Uys et al., 2012; Mohtar et al., 2013) on buyers of cell phones have revealed that practically every understudies at a school level own cell phones. Albeit the greater part of the understudies own cell phones not for discovering and instructing reason, yet rather roundabout cell phones can be facilitated to profitable and beneficial purposes. Portable development, for instance, a cell phone can change over a conventional classroom to a flexible classroom where it offers instructors and understudies to access to the teaching and learning materials remotely at any situation and at whatever point.

Kim and Altmann (2013) have coordinated a study on getting a handle on smartphones learning, improvement at Seoul National University, Korea. Their work focused on the utilization of mobile phone applications for learning among Education and Engineering understudies. Their divulgences uncovered that for the most part every understudy had 80 applications on their PDAs. 16% of the applications were used for some sort of learning.

A formed report with respect to phones among therapeutic understudies in the United Kingdom was spoken to in (Payne et al., 2012). In this test, an online diagram of supportive understudies was gotten a handle on inside of one United Kingdom social insurance area. People were asking concerning whether they have a wireless and in the event that they utilized

applications on their mobile phone to bolster their guideline. Their audit found an abnormal state of PDA possession and people got a handle on the advancement of more applications to bolster restorative understudies. Uys et al. (2012) drove a blueprint on wireless use at a South African University. The focal point of their work was to evaluate the use of phone applications for interpersonal coordinated effort applications. Revelations of their examination have uncovered that understudies passed an ordinary of five hours for consistently on their PDAs, talking with others by strategy for SNS, and stay online for around 16 hours for consistently.

Revelations of their examination have uncovered that understudies passed a conventional of five hours for consistently on their mobile phones, talking with others by technique for SNS, and stay online for close to 16 hours for consistently. The piece has guaranteed that students in Malaysia had gotten mobile phones as a prerequisite for finding at higher learning affiliations. Understudies used PDAs for sharing notes between classmates, recording addresses, and taking photos of assignments for future reference and sharing exam results on a Facebook through their phones. Jones and Heinrichs (2012) have driven a study to inspect to which degree understudies practice PDA protection. A graph of surety-related practices was created for understudies in business divisions at a run of the mill state financed schools. Their results study showed that understudies imprudent in their mobile phone securely with men more orchestrated to go on part in unsafe practices than women. Around there were no capacities in practices based upon change level or utilization of mobile phones for cash related trades.

Academicians in addition guided a study to test a social aftereffect of wireless to the social affiliation and mental achievement (Park and Lee, 2012). The work was coordinated over a few colleges close to the metropolitan areas in Korea. A sum of 339 respondents partook in the study, and data from 279 understudies were associated for the examination (97 individuals and 182 ladies). The more noteworthy segment of the individuals asserted and used cell phones reliably. To review the associations between cell phone uses and success, the study began by portraying the prerequisites of an understudy that are executed by a cell phone. The aims of cell phone use were managed by requesting respondents how well each of the declarations identified with their own specific point of view of cell phone uses (1 = not under any condition; 5 = accurately). The revelations have set up a colossal connection between

solid associations and cell phone use for mental flourishing. Their revelations moreover prescribe that a cell phone can work as a stage through which understudies can associate with others, along these lines adding to upgrading enthusiastic and mental.Venkatesh (2010) noted that buyer practices are fundamentally socio-cultural wonders that should be examined in socio-cultural terms. He stressed cross-cultural studies ought to contain no less than two unique societies as a feature of the same field study, despite the fact that it is conceivable to lead a relative study utilizing a solitary social setting and establish correlations with different societies utilizing printed data instead of domain data. He additionally clarified that cross-social studies might fuse cross-national examinations which concentrates on variables that are targeted measures that need no cross-cultural interpretation. Concentrates on the field of mobile telephone innovations are just as of late showing up.

Issac et al. (2011) examined telephone use in social contexts in two created nations – United States and France. Their examination concentrated on the mobile phones used as a component of social scenes, the imprint of the worthy use of mobile phones in social contexts. They centred on whether the utilization and diminish identified with the use of mobile phones shift by nation. Their overview demonstrated critical contrasts between clients in the United States and France when it came to utilizing phones as a section of open boulevards or while pushing an auto. French clients had an entirely negative perspective of using mobile phones while driving, this might be ascribed to the direction that it is illicit in France to drive and chew the fat on a phone at the same time. Fluctuations were additionally found out in the utilization and states of mind toward the usage of mobile telephones for both voice calls and message informing. French customers will probably utilize content informing in every one of the situations considered with the exception of while driving. The scientists clarified that, a percentage of the distinctions might be credited to social and legitimate contrasts between these nations, unlike variables, for example, age or the time allotment that somebody has used a mobile telephone might be decisive.

Carlson et al. (2010) examined the hierarchical conduct angle by watching the effect of mobile phones on choice making in deals strengths inside of associations in United States and France. They called back about the distinctions in deals power conduct. Relationships were directed to

compute out if the nation, time allotment the innovation has been employed, or their associations were the significant impact. Their work showed that new innovation appropriation was in charge of a shortening of choice setting aside a few transactions in both lands. And so again, contasts in institutionalization, formalization and choice setting aside a few minutes were marked. The aftereffects of the subject established that social contrasts between nations represented a big helping of the eminences.

Hofvenschiold (2010) studied the impact of social foundation and word related status in transit individuals' interface and experience innovation. She reviewed college students and youthful experts from Germany and the United Kingdom to think about the state of mind to and utilisation of mobile telephones. Contrasts in states of mind were quantifiable when enthusiastic and motivational functions of mobile telephone use were investigated.

Castells et al. (2010) created a point by point arrangement of existing examination confirmation of the social functions of remote correspondence innovations including mobile telephones. They showed social contrasts in correspondence style inclinations affected the response rates of remote innovations. The scientists planned to inspire general examples for the social separation of remote dispersion in various social orders of Europe, America, and the Asia Pacific locales. They cite to various studies demonstrating that content informing is more predominant among the adolescent crosswise over the states. Different discoveries incorporate the high occurrence of phone-borrowing in parts of Europe; effect on trek arranging in explorers and mobile laborers; prevalence of mobile Internet in Japan; mobile telephone as augmentation of individual character in Japan; and use of phones for correspondence and as materialistic trifles by transient specialists in China.

Castells et al. (2010) broadly investigated the rise of the mobile youth in a cross-cultural point of perspective. Their expressed speculation was that there is an adolescent culture that encounters in mobile correspondence a sufficient type of construction and fortification. They show that a cracking percentage of the examination into this adolescent society has focused on Europe. The scientists refer to confirm for the development of aggregate character coming about because of peer-grouping in view of arranged amiability. They inspect proof in the United States where owning a mobile phone for an adolescent has become into a soul

changing experience. This accumulation raises a broad variety of remarkable society properties for each of the countries or areas contemplated.

Most past composing has moved nearer the mobile phone as a novel development, still in its gathering and design phase. Research looking at in front of calendar use is abundant, both in association with steady (voice) phone use and SMS use. The diagram stage sees also provoked an a lot of examinations on comfort, menu arrangement and ergonomics (Barkhuus countless have taken a gander at mobile telephone use designs as identified with clients' regular lives. For instance, Palen et al. (2009) got a gander at new mobile telephone clients' practices and their changing impression of social distance. Ito et al. (2008) got a gander at mobile telephone use and usefulness, yet among young people, a gathering with various demands and money related means than working adults.

Despite the fact that the accessibility and along these lines, utilization of advanced cells has as of not long ago been constrained, the imminent of mobile data and connection mindful gadgets have brought about various examination investigations of conceivable future employments of mobile individual gadgets all in all. Sohn et al. (2008) for instance saw the mobile data needs of members and found that 30 percent never received their mobile data need fulfilled.

Bacchus and Polichar (2010) have taken a gander at how willing people are to share touchy data, for example, their area, with whom they would willing to divvy up this data and under what conditions.

Bell and Dourish (2009) suggest that universal registering has as of now happened, nonetheless in a structure unique in relation to that initially imagined. They highlight that Weiser's situation does not hold the idea of the bore gadget (e.g., individual multifunctional mobile phone) and proceed ahead to describe events in which the mobile gadget is utilized every bit a part of ways that may portray the genuine yet chaotic ubicomp. However, it has not been clear how this case shows itself in more well informed situations, or what this implies all the more for the most part to ubicomp's vision and future.

2.1.1 Gender based on Mobile Phone Usage

Numerous works have taken a gander at mobile phone use amongst college students in several nations (Baron and Campbell, 2010; Beaver et al., 2010; Hong et al., 2012; Ling and Horst, 2011; Balakrishnan and Raj, 2012;; Lobo and Joshma, 2013; Suominen et al., 2014; Walsh et al., 2010; Ogunyemi, 2010).

According to Beaver et al. (2010) people of understudies in the USA are more strained over their daughters' wellbeing than they would be for their kids, in this way people may be more immovable that their daughters convey a cellular phone at all times. Security was seen to be a foremost inspiration driving why females use cellular telephones in Malaysia (Dresler-Hawke and Mansvelt, 2008) and New Zealand (Balakrishnan and Raj, 2012), and notwithstanding help them not feel melancholy (Dresler-Hawke and Mansvelt, 2008). Female understudies in Malaysia and Australia use their telephones as a security contraption, to contact others when they are in hazard (Balakrishnan and Raj, 2012; Walsh et al., 2010).

Aristocrat and Campbell (2010) touched on strange, however effective frameworks that Swedish female understudies use cell telephones for with a particular deciding objective to keep themselves secure. Given females more paramount physical defencelessness in encounters with an outcast, the experience could be avoided by asserting to be immersed on her cellular telephone.

An overview on the fulfillments of cellular telephone use by Grellhesl and Punyanunt-Carter (2012) demonstrated that female undergrads in the USA scored higher than folks in the pleasure of cell telephones for loosening up and escape. The female understudies equivalently scored higher than male understudies in the total joy from cellular telephone use, demonstrating that female understudies feel more grounded ties to their cellular telephones than male understudies. The study found that female undergrads from the USA will likely have dialogs over cellular telephones more routinely (Baron and Campbell, 2010; Beaver et al., 2010), and Malaysian female understudies have lengthier examinations than male understudies (Balakrishnan and Raj, 2012). Male understudies in the USA and Malaysia

generally make calls to get ready outlines, whilst females will most likely make requires a social visit (Balakrishnan and Raj, 2012; Grellhesl and Punyanunt-Carter, 2012).

Ogunyemi (2010) noticed that African male understudies living in the UK need to message to show kinship whilst the female understudies like to draw a call rather than a substance. Beaver et al. (2010) and Baron and Campbell (2010) both agree this is because of the women are more relationship arranged than folks, and along these lines use cellular telephones to advance social collaboration.

Mehrotra and Nguyen (2012), who did a study in Rwanda, watched the converse to be genuine. They added to that men put more essentiality in talk over a cell phone for reliably than the ladies do, with ladies passing the more prominent voice of their talking time in the midst of the night. Despite the way that by far most of the illustrations utilized as a part of the study were of a more arranged age pack than understudies, Rwanda is still a to an awesome degree young nation in general terms whereby the cellular phone gathering rate amongst the ladies is low.

Research made in the USA and Malaysia found that female undergrads will presumably stay in contact with their relatives, to share experiences and search for eager monetary backing. While male undergrads simply contact their gatekeepers to keep them merry (Balakrishnan and Raj, 2012; Chen and Katz, 2009). But male understudies from the USA use cellular telephones less in examination, they were set up to hold part in computer games essentially more frequently than females, which may realize male understudies contributing a more noticeable measure of vitality in their cell telephones (Jackson et al., 2010).

Respectable and Campbell (2010) indicated that female understudies in the USA were conceivably more exasperates by reachability, since female understudies send and get more texts than male understudies. Male understudies in New Zealand will likely use content educating to make new contacts than female understudies, whilst female understudies pervasively used substance illuminating for talking with dear friends and family.Outstandingly, Wilksa (2008) took a gander at sex and utilization styles, (for example, rashness, pattern awareness, innovation excitement, thrift, environmentalism) among youthful

mobile telephone clients in Finland. In addition, Wilksa found that telephone use designs split not along sex, but rather along utilization style. Less studies have taken a gander at the individual effect of email-empowered phones, for instance Mazmanian et al. (2009) and Middleton and Cukier (2009), who discovered broad troublesome impacts of Blackberries on clients' everyday lives, in spite of clients' conflicts that the gadgets made them more effective, brief and beneficial. At final, different studies have looked at utilization of particular voices of more up to date multifunctional phones; O'Hara et al. (2009) studied the use of video correspondence, and Karlson et al. (2009) explored sharing practices of modern mobile telephones.

Kindberg et al. (2009) took a gander at mobile picture sharing, and Nylander et al. (2009) concentrated how phones with Internet access are being utilized and demonstrated that a substantial component of Internet access from mobile gadgets actually happens in circumstances where the client had Internet access through different means, for example, a PC.

2.1.2 Age based on Mobile Phone Usage

The mobile phone has been distinguished by its pervasive nature since its inception and bears nowadays reversed into a regular device for some individuals (Fowler and Noyes, 2015). Proprietorship and utilization of mobile phones are more common in youngsters (Baron, 2010).

Smartphone use continues on spreading out amongst all ages, especially by the under 25 year olds. Ofcom statistical data points for the UK demonstrate that 61% of grown-up clients claimed a smartphone in 2014 and 93% had a mobile telephone (Ofcom raw numbers, 2014).

According Fowler and Noyes (2014) it has been projected that the intentions behind the accomplishment of the mobile telephone are because of its convenience, multipurpose function, consistent availability and reachability. The last has prompted terms, for example, dependably on and ceaseless contact as a method for describing the way clients associate with this invention. In that respect is probably the mobile phone has affected individuals' lives.

Brown (2011) remarking on a behavioural study by Motorola supports the effect mobile innovation has had on individuals' lives of forever changing the way we play, live and adore. It has been insisted that mobile phones are rethinking professions, the family unit and social dealings. The mobile telephone encourages individuals in the association of their lifetimes.

Ling and Ytrri (2002) presented the terms miniaturized scale coordination and hyper-coordination to comprehend the way clients compose their lives through utilizing their mobile phone. Small scale coordination alludes to the adaptability that can take place with a mobile telephone while organizing gatherings; it is conceivable to change and adjust the Ascension as the need emerges accordingly the when and where of gatherings can be modified through the mobile phone. Hyper-coordination alludes to smaller scale coordination and the expressive utilization of the mobile for social and enthusiastic agreement. This availability from hyper-coordination alludes to work, family and private connections.

Geser (2006) has recorded the regularly expanding utilization of the mobile telephone by youthful clients and the implication of the content informing society. The quick increment in mobile telephone usage has been tested in numerous studies furthermore the formation of a mobile telephone correspondence society.

Madell and Muncer (2004) found that the most imperative uses for mobile phones amongst adolescents were for making and accepting calls and messaging. They also investigated the states of mind of college students towards talking via-à-vis, messaging or approaching the mobile. Content informing was brought into the field of correspondence innovation nearly unintentionally. In 1982, a voice, mobile phone system that would run all through Europe was hit by a multinational European activity known as Group Special Mobile, or GSM. This came into operation in 1992. A trace of remaining data transmission was made accessible with the goal that clients could create short messages on the keypad by tapping the number keys somewhere around one and four times to deliver alphabetic characters. This was SMS (Short Message System) messaging and rapidly grew to be well known amongst youthful grownups and teens. One of the central factors that have been discovered in numerous investigations of mobile phone use and conduct in grownups and youngsters is that the very work that

individuals appreciate from utilizing their mobile telephone is additionally the very work that causes a negative slant to them.

2.2 Mobile Phone Security

Audrolidakis and Kandus (2011) reported that a late published survey in November 2008 concentrated on mobile phones, security issues and to the extent to which these publications concern the clients. The conclusion was that a noteworthy portion of the members were amazingly worried about security and conceivable 3d party unapproved access to their private data. They saw the bizarre conduct among mobile telephone clients, who at times knew about the dangers that they could be introduced to yet does not respect fortifying the security of their telephone to be a basic fear. Advertisement they additionally gave a fair justification for this watched conduct, expressing that mobile phone clients are uninformed of the steps that ought to be required to keep a strategic distance from conceivable security ruptures. Mindfulness battles went for enhancing client learning, states of mind and conduct towards data security were utilized as the interventions as a function of this action research study.

Aoki and Downes (2010) counted the gatherings as the cost-conscious bunch, wellbeing/security cognizant, needy, complex, and pragmatic clients. The cost-conscious clients trust that a mobile telephone offers them some assistance with saving cash. The wellbeing/security cognizant clients are perceptive of their own security and having a smart phone gives them a sentiment security. The subordinate client is a human who is strung-out on his/her phone and feels disengaged to the universe without one. The refined clients have received their phones for a very long time and feel it is totally a need for fermenting along the planet. The handy client trusts a mobile telephone gives cost sparing, security advantages, and time effectiveness. This work serves as a profitable rule on how polls concentrating on mobile phone use might be outlined by utilizing centre meetings. The worldwide means of mobile advancements makes the cross-cultural investigation of the behavioural properties of mobile telephone utilization a point of current premium.

Talib et al., (2010) expressed that little confirmation exists to indicate that mobile phone clients are educated about, or are actually honing, data security.

Kruger and Kearney (2006) acknowledged the significance of surveying the effect of a mindfulness battle. In their journey to decide a worldwide mindfulness level of the tie-up, they picked out an arrangement of angles identified with what customers know (learning), think (demeanour) and do (behaviour).

Tsohou et al. (2012) considered it to be a consistent exertion as far as which groups of onlookers' consideration is put forward with regard to data security and its significance and then as to empower security-situated conduct in them.

Becker et al. (2011) reported that savvy gadgets are interested in both customary and mobile particular dangers because of the various parts shrewd mobile gadgets play and the heterogeneity of mobile correspondence innovations and organized administrations.

Gelenbe et al. (2015) expressed that among the conventional dangers that brilliant mobile gadgets face, we incorporate physical assaults that require physical access to the gadget, gadget autonomous assaults, for example, spying on the remote medium or principle the-centre assaults, email-based spam and phishing, and IP based assaults.

Wahlisch et al. (2013) called attention to that present IP-construct assaults experienced in light of mobile appliances have been observed to be to a large extent like those on non-mobile gadgets, even so we are more inspired by the characteristics of assaults that are custom-made specially for mobile appliances. With the growing prominence of keen gadgets, mobile specific dangers have advanced from SMS/MMS-based foreswearing of service assaults to more refined assaults that more frequently than not come as malware and target both the core system and the mobile clients.

Zhou and Jiang (2012) reported that the capacity of savvy gadgets to present and move applications from authority markets as easily as from obscure sources opens them to malware keeping in mind the mobile malware risk is not fresh, it is unmistakably advancing and developing as assailants examination with new designs of action by focusing on mobile users.

CHAPTER 3
THEORETICAL FRAMWORK

3.1 Self-Efficacy on Mobile Phone Usage

Mobile phone innovations are presently in the hands of very nearly 31% or 2 billion individuals of the 6.47 billion individuals on this planet (Motorola, 2010). The infiltration of these innovations is expanding quickly with around 779 million (Gartner Press Release, 2010) mobile phones sold each year and anticipated that would reach more than 1 billion units for every year sold by 2009. These stunning numbers are pointer of the development and scope of mobile phones. Asia is the fastest-growing locale, represented one of each four phones sold in 2005, a pace that is anticipated to increment to one of three by 2009 (Gartner Press Release, 2010). The most recent information from March 2006 demonstrates that India is the quickest developing mobile business sector on the planet with more than 5 million new clients included every month, bringing the aggregate to more than 90 million clients (Telecom Regulatory Authority of India official statement, 2012). However, this speaks to just around 8% of India's evaluated downright mid-2005 populace (Population Reference Bureau Statistics, 2010). The comparing US information from December 2005 demonstrates that there are 207 million mobile clients in the US (CTIA Semi-Annual Wireless Industry Survey, 2010).

Townsend (2010) said that the dispersion of the mobile telephone was among the speediest of any innovation ever. Such a quickly developing and across the board correspondence innovation and medium has imperative social settings and suggestions. Aoki and Downes (2010) noticed that mobile telephone use in social settings has been a less examined range when contrasted with the exploration of the building and arrangement parts of mobile innovations. McGuigan (2012) called attention to that it is very hard to discover the basic exploration which investigates the social worth and social motivation behind mobile phones. Just as of late, research has distributed on how individuals use mobile phones in their everyday life. Then again, a larger part of these studies have concentrated on considering populaces inside of a generally homogeneous society. Weilenmann et al. (2010) directed field investigations of open utilization of mobile phones among adolescents in Sweden. Their study shed light on how the mobile telephone has come to be utilized as a device for neighborhood

social collaboration, instead of just as a gadget for correspondence with separated others. Their perceptions pointed towards the community oriented nature of mobile telephone use. The scientists inspected how the phones were shared and how their field information could be useful while outlining new mobile innovation and administrations for the adolescent.

Katz (2010) investigated the conceivable impacts of remote correspondence on individuals' lives. He recognized a few levels of impacts of such an innovation. The first-order impacts are immediate impacts that are instantly seen by clients, they incorporate vulnerability diminishment, individual security, and individual productivity. The 'second-order impacts are roundabout impacts which speak to the encounters or sentiments that individuals have or might see in others, they incorporate more tightly coupling of household creation, data instantaneousness, and contractibility. The third-order impacts are the minimum direct impacts that are watched not by clients of the innovation, but rather by outside eyewitnesses who concentrate on the impacts of the innovation on the general public when all is said in done, they incorporate social communication, social control, and creative uses or unexpected utilization. Mobile phones are rethinking and obscuring the line in the middle of open and private spaces. Cooper (2012) specified that individuals out in the open space might be out of the blue presented to the other side of a two-party private collaboration, which can be baffling with hypotheses about the missing side of the association. Fortunati (2012) noticed that mobile phones supported the dynamic infringement of closeness in a general society circle.

Palen et al. (2010) has investigated this issue and the view of mobile telephone utilization in people in general. They contemplated the conduct of new mobile clients over a time of six weeks after procurement of phones. Utilizing interviews and voice-mail, their study noticed that examples of mobile telephone utilization changed after some time and there was a huge deviation between the user-predicted uses to their real use. The specialists additionally concentrated how the view of mobile telephone use in broad daylight settings changed over the length of time of the study. At first, the recognition was overwhelmingly negative. Be that as it may, they noticed that new clients over a timeframe turned out to be additionally tolerating of the utilization of mobile phones out in the open spots. Their study discovered individuals at first embraced mobile phones for wellbeing/security and business or job-related

reasons rather than social reasons. Be that as it may, about all subjects in their study reported the utilization of their mobile phones for social collaborations had become over a time frame. These corporations may not be the conventional voice based connection. Puro (2012) noticed that Finland has one of the most noteworthy mobile telephone densities on the planet, coming to more than 90% of the general population under 30 years old. Taylor and Harper (2010) noticed that youngsters use content informing on mobile phones as types of blessings to concrete social connections. Aoki and Downes (2010) concentrated on the behavioural and mental parts of mobile telephone utilization among undergrads. They attempted to discover the purposes for why an innovation is received particularly. They recognized a few attitudinal variables in the view of the exploratory study, including, need in present day times, cost effectiveness when contrasted with landline telephones, wellbeing or security, and reliance. The concentrate likewise tried to take a gander at the motivational and behavioural qualities of mobile telephone utilization. The creators attempted to join their outcomes with the consequence of past exploration to discover the patterns of utilization by the adolescent, why undergrads in the US utilize the mobile telephone, what they think about the innovation, and how they utilize it. The motivational subjects recognized by the study incorporate individual wellbeing, monetary motivator, data access, social cooperation, parental contacts, time administration/coordination, reliance, picture, and security administration. The consequences of the centre gathering interviews demonstrated five unmistakable client bunches as far as their states of mind toward their mobile telephone use and as far as the levels of incorporating mobile phones into their lives.

The social foundation can impact the way innovation is seen, embraced and utilized. In spite of the worldwide way of the selection of mobile innovations, there are just a couple studies which have examined the cross- social perspectives. Aoki and Downes (2010) examined "the inborn inspirations for the reception of mobile phones and the behavioral qualities of their utilization" which are of enthusiasm for the connection of understudies in the US. This study will extend the past exploration to incorporate a cross-cultural correlation of college understudies in the United States and India. Knowing the inherent inspiration for embracing innovation might help in picking up a superior comprehension of why an innovation is utilized a specific path by a specific gathering of individuals. The behavioral qualities incorporate

utilization information, for example, length of mobile telephone use, ordinary time of mobile telephone use, normal number of calls got/sent, the run of the mill area of mobile telephone use furthermore the utilization and the quantity of instant messages. Mobile phones have a characteristic social impact on the way the advances stress compactness and steady correspondence. The compact way of this correspondence medium implies that they are regularly utilized as a part of open space. Individuals might be included in mobile correspondence as either clients or members in an open space with different clients. Some mobile telephone clients might grasp a resultant rethinking of their own space. While different clients might consider mobile telephone correspondence a special individual space, thus impart their mobile telephone numbers just to their dear loved ones. Cooper (2012) expressed that the utilization of the mobile in certain open spaces makes the connection of private and open somewhat distinctive. This prompts questions about the dispositions with respect to the utilization of mobile phones in an open setting. Moreover, mobile phones today go past simply voice correspondence and give a huge number of different elements and administrations, including content informing (SMS), mixed media informing (MMS), photograph show and recording, video playback and recording, calendaring, and so on. In this manner, the paper will likewise search out the utilization examples of mobile phones as a data access gadget as for these elements.

Mobile gadgets have turned into the most widely recognized method for correspondence around the entire world. According to World Fact Book (2012), the CIA made an evaluation in 2011, which shows that they over 6 billion mobile phone user in the world out of 7 billion individuals. With the fast development of correspondence system use, ruptures in system security and episodes of exchange misrepresentation are expanding. Hence, building up an exceptionally secure verification system is basic. The expanded utilization of mobile gadgets to store a lot of information conveys the danger of misfortune or burglary, which can trade off the security of data. This trade off of security is particularly unsafe when touchy individual data are included. The present confirmation strategy for the security of mobile gadgets relies on upon the utilization of a Personal Identification Number (PIN) to check the client; in any case, basically utilizing the right PIN does not ensure a man's character. Therefore, a higher level of protection is required, particularly with the developments of mobile phone devices.

3.2 Security Considerations

This talk about various security considerations in mobile phone security

- ***Authentication Strategies***

Authentication can be classified into three broad classes:

-What the client acknowledges (e.g. secret key or PIN).

- What the client possesses (e.g. tokens or Card).

- What the client is (such as Biometrics).

PIN is a mystery information validation technique and thus depends upon learning that just the approved client has. In spite of the fact that the PIN and watchword are the most ordinarily utilized techniques for verification as a part of the data system (Scott, 2010), such mystery learning approaches, shockingly have since quite a while ago settled issues, with shortcomings frequently been presented by the approved clients themselves. PIN and passwords are most plainly recorded in connection, with awful works of, including the choice of feeble and effortlessly strings that are guessable, importing passwords to other individuals, keeping in touch with them down where others can discover them, and never showing signs of change them (Alhussain et al., 2013). Thus, these methodologies are the most effortless focus of programmers (Zahidi and Hajj, 2009). A physical substance or thing that an individual has to set up individual ID, for example, an international ID, ID card, and Master card is called a security token (Alhussain et al., 2013). This token based procedure is around like the puzzle learning approach, as it generally relies on the customer reviewing to pass on along something to ensure security whereby the token ought to be physically present (Clarke and Furnell, 2010). Thus, mystery learning and token based verification methodologies are unsuitable techniques for accomplishing the security prerequisites of data systems, as they can't separate between an approved and an unapproved individual who falsely gets the information or token of the approved individual (Alhussain et al., 2013). Then again, biometric verification depends on the extraordinary physiological and behavioral qualities of a person: henceforth, it can't be overlooked, stolen or lost.

- ***Security for Mobile***

Gadgets security in mobile gadgets must have the capacity to ensure the hobbies of clients, including their protection, and additionally those of the gadget producers, system administrators, and administration suppliers. Be that as it may, mobile gadgets might contain touchy and private client information; thus, burglary and loss of mobile gadgets are turning into a significant issue and the requirement for cutting edge client confirmation in mobile gadgets is getting to be crucial. Moreover, as mobile gadgets get to be more astute and bolster more information capacities, mobile makers are confronting a large number of the same dangers as PCs, to be specific, pernicious programming assaults. The present security system for mobile gadgets depends on the utilization of a PIN which has a few shortcomings. Security from the unapproved use can all the more adequately be accomplished by more propelled client validation systems (Alhussain et al., 2013).

- ***User Authentication in Mobile Networks***

As to client verification, mobile system suppliers are for the most part worried with the false utilization of their system; along these lines, the confirmation components are intended to guarantee that just honest to goodness gadget interface with the system. For instance, GSM systems approve the qualifications in the SIM card. In addition, there are no procurements in 2G mobileular systems to confirm the system to the client system. This permits man-in-the-centre assaults where an aggressor can control low-gold hardware which reproduces a remote system and can gain the certifications of the client. On the other hand, with the security upgrade of UMTS, most mobile gadgets for both GSM and UMTS take into consideration gadgets to be arranged so that the client must enter a PIN before utilizing the gadget. Yet, the client can without much of a stretch debilitate this system (Alhussain et al., 2013). Along these lines, the security for both GSM and UMTS mobile gadgets depends on a PIN methodology which is under-used and can, thusly, be considered to give deficient insurance in a few cases.

3.3 Mobile Operating System

A standout amongst the most broadly utilized advancements today is mobile innovation. It incorporates a few or we can say all types of versatile innovation such as portable

workstations, palmtops, mobile phones, individual advanced partners, remote card installment terminals, worldwide situating systems. This innovation has profoundly expanded the world over step by step. This can be obviously found in our everyday life as a needy person likewise either have a cellular telephone or has admitted to it. It has changed the method for working together. Already individuals used to go to banks or workplaces to do their errand, however now they can without much of a stretch do it from cellular telephones. It can be seen that in the previous couple of years the remote advancements are profoundly created. Alongside the exponential change in the execution and limit of remote correspondences systems, the data can be effortlessly gotten to utilizing mobile gadgets. So as to enhance their base and taking off information scope, the mobile systems are spending a substantial sum. The ceaseless development in mobile innovation is affecting everybody's life. The clients are getting profited from the advances in mobile innovation (Sharma et al., 2013). This is unmistakably noticeable in our everyday life. Already, keeping in mind the end goal to mail, imperative records one needs to convey it from way to entryway yet with the progression in mobile innovation one can without much of a stretch send it in a couple of minutes as delicately duplicate. Truly, the utilization of advanced cells and tablets has changed interchanges and stimulation. The development in mobile innovation is influencing different fields additionally like it is assuming a fundamental part in social insurance systems. As a sample, if a man possesses a business, then he is allowed to extend his business instead of restricting it to a specific region. This can be seen from the before year that with the amplifying number of years the scopes of convenient are likewise developing. The season of a mobile phone is tended to by 'G'. From 1946 to 1980, 0G i.e. the zero period won. This included early cell phones which were particularly absurd and it must be utilized as a bit of autos, trucks and envelope cases. It had a voice call highlight just. After 0G forefront came which is 1G i.e. exceptional. In this period cell phones were fundamental gadgets which wear down AMPS/Datatac improvement. Its portions were voice calls with constrained information which was to some degree higher than the past time. As the time passed the going with modernized period showed up which is the 2G i.e. the second period adaptable structure. Its parts were truly improved than the past periods. It had voice, SMS and circuit exchanged information highlights. The advances which won amidst this period were GSM, iDEN, EDGE, GPRS, CDMA, TDMA and HSCSD. Out of the above headways some have a spot with the 2.5G gages group. With a specific end goal to

show new portions and advancements, the cutting edge was shown i.e. 3G. It had unrivaled parts like broadband information, voice and spilling video, however this improvement was not completely executed (Sharma et al., 2013). It came into light from 2004 which included movements like W-CDMA, 1Xev-DO. Additionally, some new fragments in the past alteration of the period, 4G were presented. This period had speedier broadband for information and visual driven data which is fit for transmitting information at 100mbps while moving and 1Gbs while stopping. On the reason of the development in compact progression, the working system on which these works can be depicted underneath near to the examination between them:

- ***Windows Phone 7***: It is conveyed by Microsoft that was utilized as a bit of cellphones and flexible contraptions, regardless, is in fact beginning now wiped out to centered markets. Windows Mobile 6.5 is the present and last shape. It depends on upon the Windows CE 5.2 piece. It is redone in C++

- ***iPhone OS (iOS):*** This solid yet excessive working system is made by Apple whose area tongue is C. It is in addition utilized as a bit of iPod touch, iPhone and iPad.

- ***BlackBerry OS:*** Research In Motion developed the working structure for its BlackBerry line of portable gadgets cellphone. It gives supports and multitasking specific data contraptions that have been gotten a handle on by RIM for use in its portable particularly the trackwheel, trackballs, touch screens and trackpad. This working structure is shaped just in C++ and it strengthens different dialects like UK English, French, US English and so forth.

- ***Symbian OS:*** it was set up in June 1988 and the working structure which depends on after fascinating Personal Digital Assistants (PDAs) from Psion is passed on by the thing improves and Symbian Ltd is the supporting affiliation. It was set up in June 1998. C++ is the nearby vernacular of Symbian OS and in this manner it is said to be known as its essential language for programming. That and moreover, it has the best introduced base. This working framework is utilized as a bit of Nokia mobiles. From the perspective of programming change, it must have the advantage Integrated Development Environment and SDK device of our decision. An Integrated Development Environment by and large has an administrator source,

interpreter, debugger and debugger, and is an application item that permits the PC planner to make programming for a specific stage. Code Warrior, Carbide C++, or Visual C++ is the Integrated Development Environment required for Symbian OS.

- ***Android OS:*** This is a thing stage and working framework for adaptable gadgets which is made by Google and it depends on upon Linux bit yet later on by Open Handset Alliance. Its neighborhood vernacular is Java, which is the formal fortified tongue. This application can be shaped in different vernaculars also in any case; later on it is assembled to neighborhood code of ARM. This OS is utilized as a bit of Samsung, HTC mobiles.

3.4 Mobile Malicious Software

The term malware is a combination of two words: malicious and software. Malware, as the name suggests any software program with malicious intention (Lawton, 2008). In general the malware is designed to execute malicious code once it is installed, and ultimately causes havoc on mobile phone devices, which sometimes rendering them unusable. Below are the main categories of malware popular for smart-phones:

3.4.1 *Viruses*

A virus is a software code with malicious intentions, which runs on the phone's background without the knowledge of the user. As soon as the virus is installed, it starts to replicate itself and occupies the memory space and resources. Viruses need a certain kind of activation, like running a program, and they have been used for a long time as a successful attack vector so as to infect Smart-phones and then spread throughout the mobile networks. Mobile viruses possess the potential to make extensive damage on Smart-phones and have been known to steal confidential data, bring mobile networks down, result in the denial of service, and drain out the power of the battery. Mobile viruses usually depend on SMS/MMS and Bluetooth to infect Smart-Phones and widely spread damage to other devices on the network. Some of the mobile viruses that have used SMS/MSS and exploited Bluetooth vulnerabilities to spread are Commwarrior and Mabir (Jiang, 2011).

3.4.2 *Worms*

A worm is similar to a virus in terms of its purpose and behavior, but the worm is self-replicating. In other words, in order for a worm to execute its malicious code, it does not need the user's intervention as it targets security flaws in the operating systems or applications and uses that security gap as a conduit to spread to other systems and applications. Recently, studies have shown that worms usually use Bluetooth as an effective mechanism for infection to launch attacks on Smart-Phones (Felt et al., 2011). Cabir, Mabir, and Commworrior are examples of worms that infected Smart-Phones through the Bluetooth interfaces, and they were able to disrupt the operating systems of the phones and drain out the power of the battery. The hazard of mobile worms stems from their capabilities of propagation and the damage they can cause when they infect a system. For instance, if a worm compromises the operating system of a smart-phone, it can make undesired phone calls and also compromise confidential data of the user (Yan and Eidenbenz, 2006).

3.4.3 *Trojans*

The Trojan horse is a program that seems to be a useful and a benign program, but it hides malicious code inside. Trojans do not replicate like the other viruses and worms, but they can attack the phone's system and steal information or cause a malfunction to the device. Trojan horses normally show in the form of a benign program, such as a game or music file. After the user installs the software, it begins in executing Trojan horse payload stealthily. Trojan horses target Smart-phones and cause disruption, financial damage and loss. Supporting, Cheng et al. (2007) reported about the Trojan horse that has a target the users of smart-phone. This Trojan horse comes hidden in a text message and sends special text messages to a Russian service provider to deduct the prepaid fees of the user.

3.4.4 *Spyware*

This malicious software infiltrates the system through the commercial software programs and sends the information about the system all over the internet to the spyware originator smart-phones (Lawton, 2008). This kind of malware is considered specifically dangerous because it monitors user's activity and because it is able to send sensitive information, such as the

keystrokes and passwords, to the spyware agent, and eventually provides a financial motive for hackers that makes them design more sophisticated spyware that can bypass the traditional countermeasures represented by anti-spyware. The danger of the spyware stems from the fact that it typically shows in the form of benign software programs and in this way it can trick unaware users to install them as useful applications. As soon as they are installed, they begin to monitor the computer activity and can capture private data and thus make the users exposed to identity theft and privacy violations (hacking).

3.4.5 *Rootkit*

This type of malware is designed so as to be installed in the operating system in order to take control of the system and then compromise it in order to get root-level privileges smart-phones (Felt et al., 2011). Rootkits are hard to be detected and can create back doors and vulnerabilities in the system. Rootkits might be hidden as part of a software package to be installed in the operating system. In the course of time, it is becoming very hard to detect rootkits today because they are often capable of updating themselves once installed, making it harder for the traditional antivirus programs to detect such malicious software. Smart-phones are susceptible to rootkits and their dire consequences because of the unique interfaces and features they provide , such as SMS/MMS, GPS, and internet browsing because rootkits stealthily target the operating systems, its particularly difficult to detect them by means of using the traditional anti-malware or anti-rootkits software because these software programs run on the operating systems, which could be easily compromised and controlled by attackers when rootkits are installed on smart-phones. Therefore, rootkits emerge as one of the moist effective attack vectors to compromise smart-phones.

CHAPTER 4
METHODOLOGY

4.1 Research Model

This study, which is aimed at investigation of self-efficacy and perception towards mobile phone security amongst university students in Libya, has taken place within the frame of a control group based on self-efficacy and opinions.

The independent variable of the survey and causal comparative study includes four variables: gender, age, mobile platform and mobile phone usage. The dependent variables were the various items in the questionnaires which range from question 1 to 16.

The 1st, 2nd, 3rd and the 4th research questions and objectives of the study have taken place around a scientific system. A figurative view of the research model and the meanings of the words used are given in Figure 1.

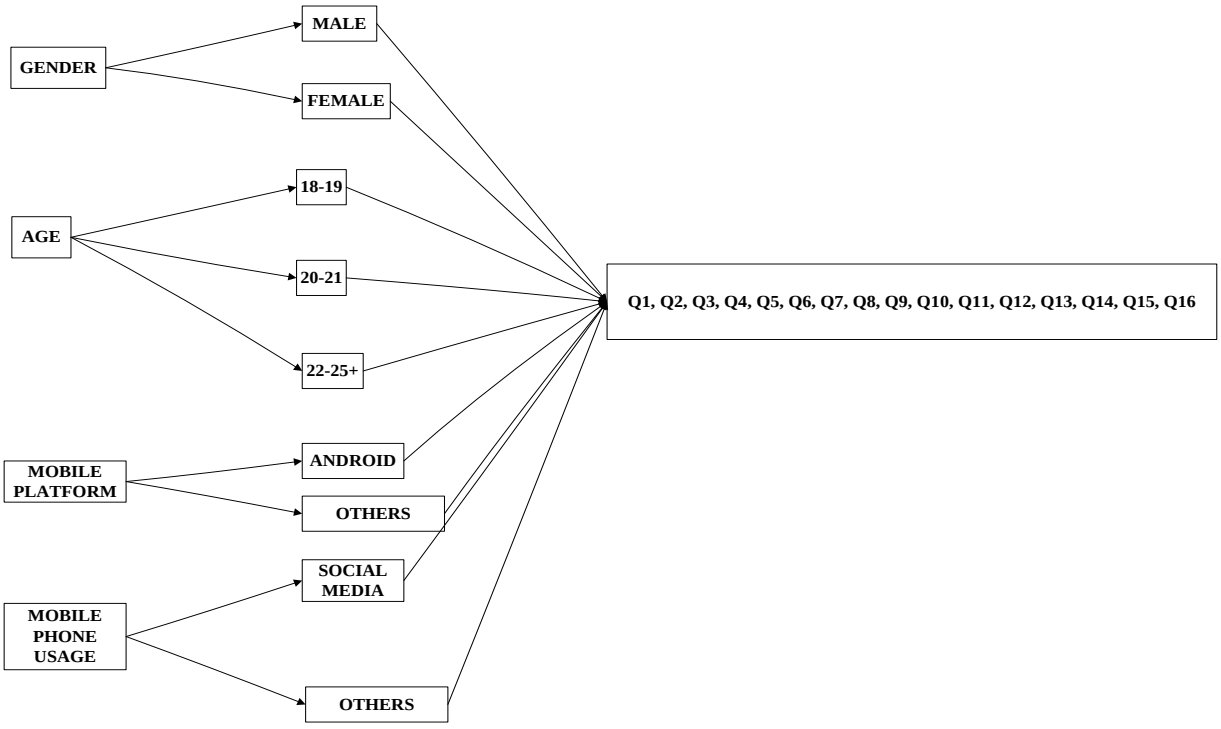

Figure 1: Research model

4.2 Participants

The volunteer participants who have mobile phones and use it were used in this study consisted of total of 557 undergraduate students from different class levels attending two different universities in Libya, which are; Tripoli University (78.46%) and Misurata University (21.64%). 190 students from Faculty of Science, 162 students from Faculty of Engineering, 50 students from faculty of Agriculture, 35 students from Faculty of Law, 120 students from Faculty of Health Science (which includes Medicine, Dentistry, Pharmacy and Nursing departments) were selected randomly. The study was conducted during the 2014-2015 Spring term. About 55.30% female and 44.70% male students participated in the survey study from all Faculties. The characteristics of the students are presented in Table 4.1.

Table 4.1: Important demographic data of participants (N = 557)

Characteristic	Frequency	%
Gender		
Female	308	55.30
Male	249	44.70
Age		
18-19	200	35.91
20-21	157	28.18
22-25+	200	35.91
University		
Tripoli	437	78.46
Misurata	120	21.64
Faculty		
Science	190	34.11
Engineering	162	29.08
Agriculture	50	8.98
Law	35	6.28
Health	120	21.54

4.2.1 Hours Students Spend on the Mobile phones daily

From the result, it was observed as shown Figure 2 below, that only 2.2% of students spend less than 1 hour daily, 5.9% of students spend 1 hour daily, 14.7% of students spend 2 hours daily and 77.2% of students spend 2+ hours daily from a population pool of 557 students who participated in the survey on their mobile phones daily. This shows that more students use more than 2 hours in a day on their mobile phones. This result was in accord with that of Lenhart (2012) who reported that understudies spend over 4 hours on mobile phones day by day. Zulkefly and Baharudin (2010) likewise reported that University of Putra students in Malaysia showed sensible measure of time and cash consumed on their mobile telephone. Braguglia (2010) reported that 41.6 % of students utilize their mobile telephone sets for around 1-3 hours on a day by day base.

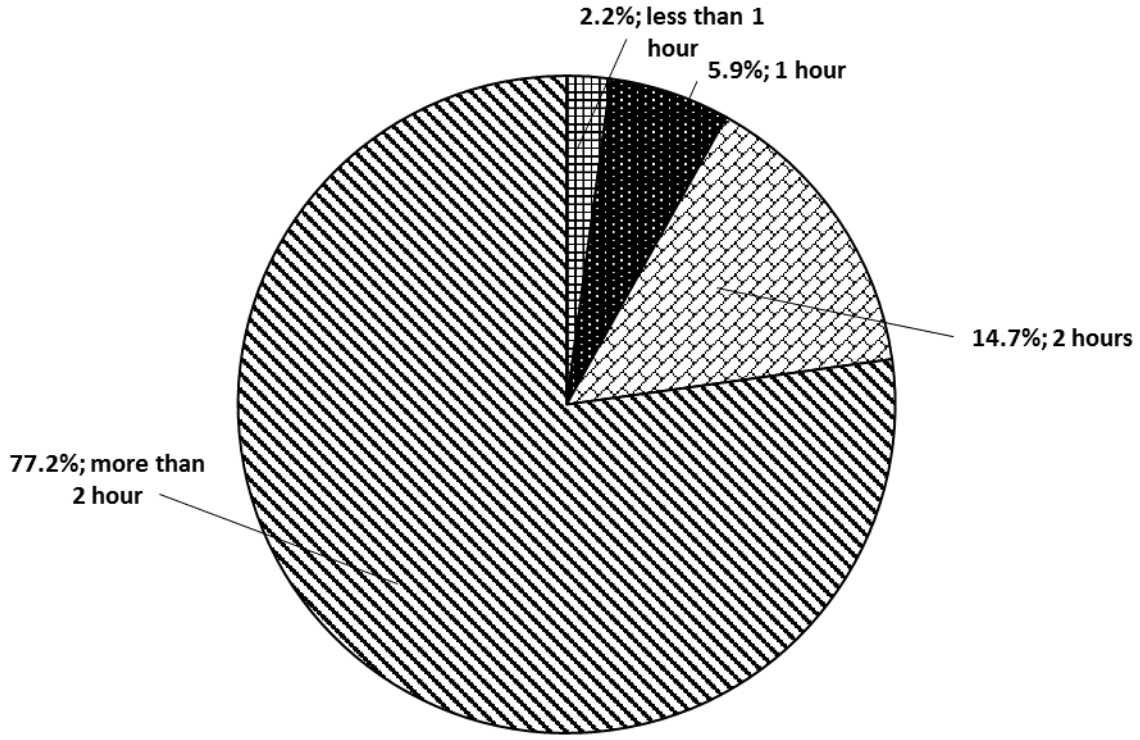

Figure 2: Hours students spend on the mobile phones daily

4.2.2 Mobile Operating System Used by Students

From the result, it was observed as shown Figure 3 below, that only 72% students use Android operating system in their mobile phones, and only 28% students use other mobile operating system such iPhone operating system (IOS) with 12%, Blackberry operating system with 9%, and Windows operating system 7%. In their mobile phones from a population pull of 557 students who participated in the survey. This shows that a lot of students use Android than other mobile operating system.

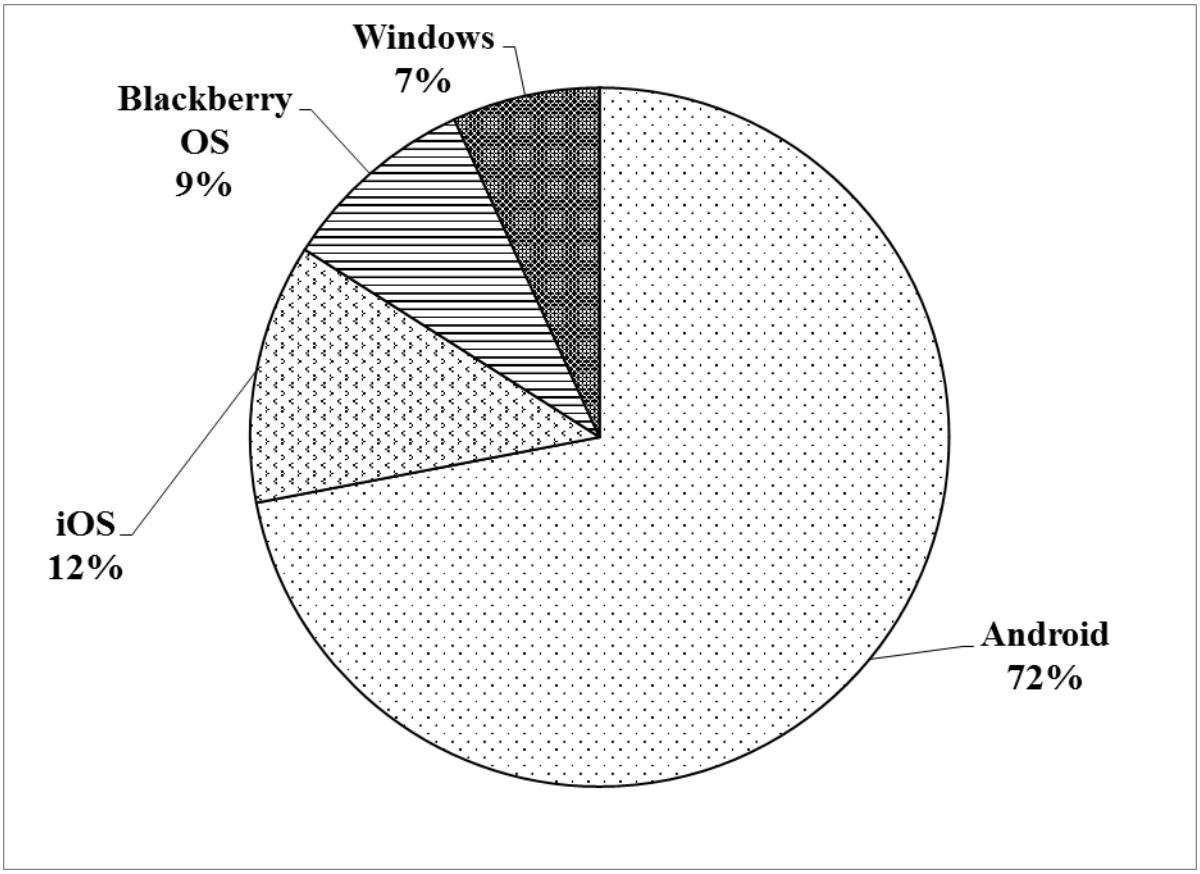

Figure 3: Mobile phone operating system used by students

4.2.3 Reasons why Students use Mobile Phone Regularly

From the result, it was observed as shown Figure 4 below, that only 81% of students use their mobile phone for regular social media purposes and 19% of students use their mobile phones for other purposes such as; watching films, listening to music, making phone calls, etc. from a population pull of 557 students whom participated in the survey. This shows that students use the mobile phones more for social media purposes and other purposes.

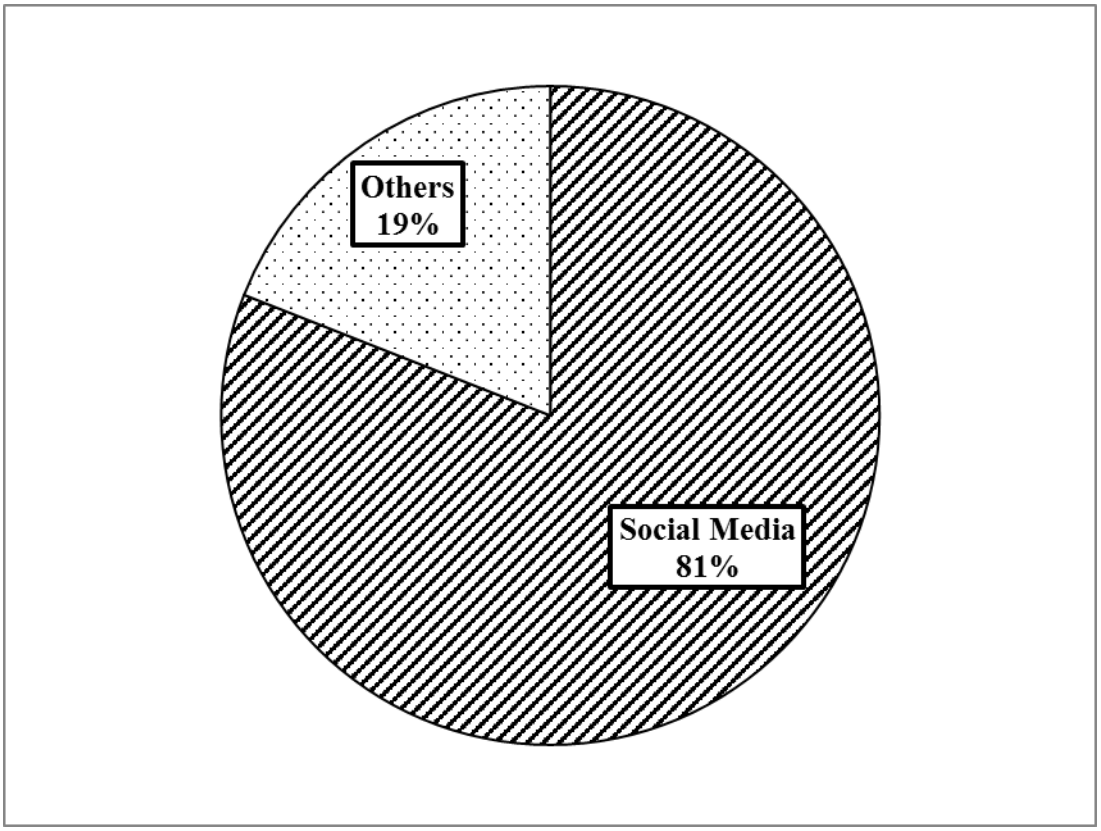

Figure 4: Reasons why students use their mobile phones

4.2.4 Antivirus Program Usage by Students on their Mobile Phones

From the result we got, it was observed as shown Figure 5 below, that only 33.9% of students have antivirus on their mobile phones and about 66.1% of students do not have antivirus on their mobile phones from a population pull of 557 students whom participated in the survey. This shows that not much of students use anti-virus on their mobile phones.

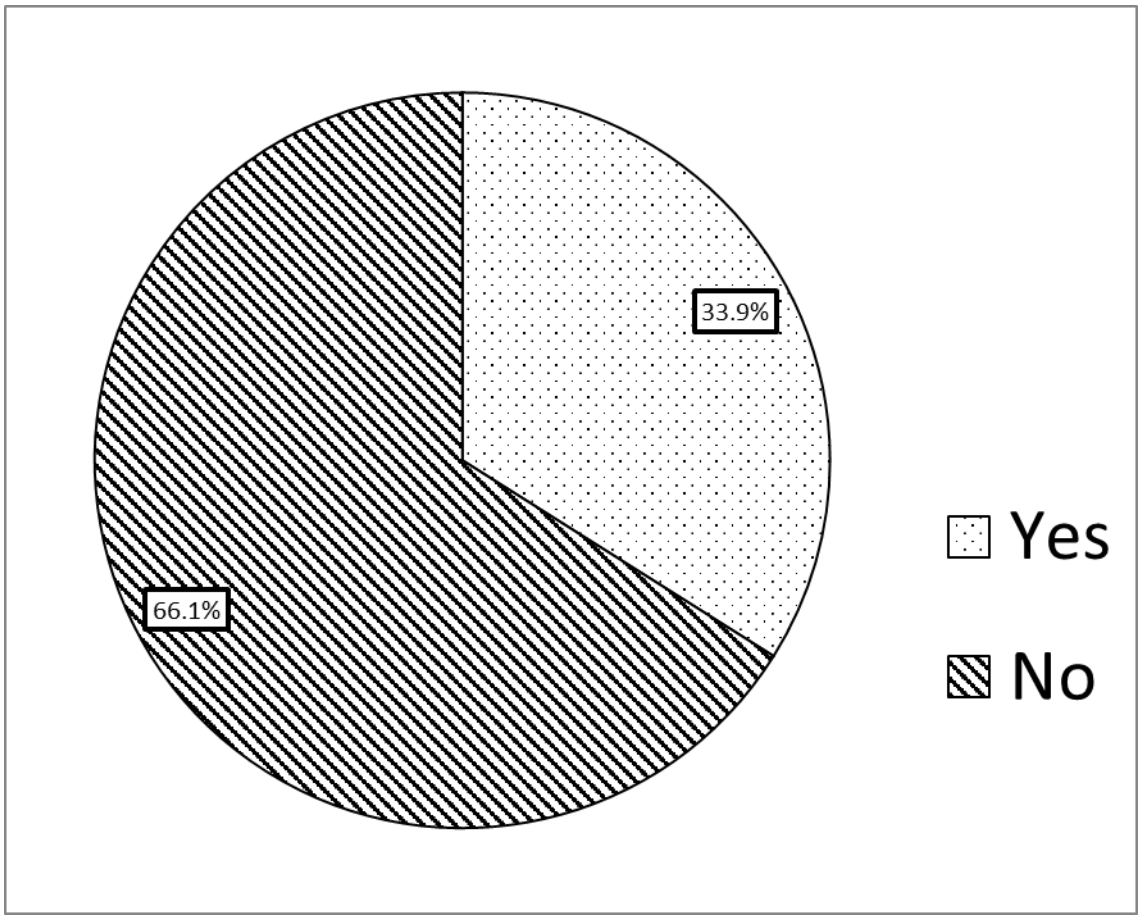

Figure 5: Anti-virus program usage by students on their mobile phones

4.3 Instruments

The developed questionnaire, which was developed by the author, under the supervision of his supervisor, is made up of 16 items in order to investigate self-efficacy of university students towards mobile phone security. The participants answered the items on 5 Likert Scale from Very Confident (5 point), Confident (4 point), Neutral (3 point), Not Confident (2 point), and Not Very Confident (1 point). The questionnaire reliability was calculated as 0.914 by using Cronbach's Alpha for 16 items. The co-efficient of reliability of all items are above 0.70 and based on this result, it was decided that the scale can be used since reliability measurements gave good acceptable results (Sipahi et al., 2010).

4.4 Data Analysis Methods

Questionnaire was used to collect data and was analyzed and interpreted using SPSS 20.0 version. Frequency and percentage, Independent sample t-test, ANOVA, methods were used during the analysis process.

4.5 Procedure

This study was designed in order to fill the gap in the university students' self-efficacy towards mobile phones security in Libya. Therefore, for this study to be successfully carried out questionnaires were given to over 700 randomly selected students in various universities in the country for over 1 month, but only 557 questionnaires were completely filled and used for the study. Questionnaires were given to students in Tripoli University, and Misaurata University and collected back from volunteering students every day for over 2 weeks. The questionnaires were given to students in different locations, such as the classroom, the faculty building, the cafeteria, etc.

After the collection of questionnaires, the accumulated data were subjected to various analyses such as; frequency and percentage, independent *t*-test and one-way ANOVA in order to give answers to the aim of the research questions of the study. Afterwards the results of the data analysis were discussed in details and conclusion and recommendation, were drawn from the results of the study.

CHAPTER 5
RESULTS AND DISSCUSSION

5.1 Self-Efficacy of University Students towards Mobile Phone Security

In order to understand the opinions of the university students' self-efficacy towards mobile phone security descriptive analysis was employed. From the result shown in Table 5.1, the mean range of the item 13 is "to be able to use the e-commerce securely" (M = 3.42; SD = 1.09), this is possibly because there are a lot of malware that might steal the credit card details of the students, which is the least mean value followed by. "To be able to differentiate normal e-mails and spam mails" (M = 3.46; SD = 1.36) and "to be able to report stolen or lost mobile phone with owner details" (M = 3.54; SD = 1.35), this is possibly because there are no direct mobile phone selling companies (such as Samsung, iPhones, etc.,) but rather just mobile selling shops/offices around the university. The highest mean values are "to be able to disable wireless access such as Bluetooth and WIFI when not required" (M = 4.17; SD = 0.94) followed by "being able to password protect, secure data stored on the phone" (M = 4.08; SD = 1.19) and meanwhile "to be able to logout when the device is not in use" (M = 3.89; SD = 1.25) which gave the highest mean value out of all items. These following items that recorded high mean might be because of the most used features of phones, because basically almost all students use their phone to browse via the wireless or data packet, they also use their phone to send or receive files via Bluetooth, mostly almost all students use passwords on their mobile phones and finally they possibly leave/logout of their phone when not in use.

Table 5.1: Self-efficacy of university students towards mobile phone security

Items	Means	Std. Deviation
1.To be able to know when a message containing a virus is received	3.79	1.26
2.To be able to create a strong password for starting to use the mobile phone	3.69	1.12
3.To be able to know how to password protect my mobile phone	3.59	1.16
4.To be able to install latest security updates	3.62	1.78
5.To be able to set auto-lock timer on mobile phone	3.65	1.11
6.To be able to report stolen or lost mobile phone with owner details	3.54	1.35
7.To be able to change the password from time to time	3.73	1.73
8.To be able to disable wireless access such as Bluetooth and WIFI when not required	4.17	0.94
9.To be able to password protects secure data stored on the phone	4.08	1.19
10.To be able to logout when the device is not in use	3.89	1.25
11.To be able to set encryption on personal and important files	3.71	1.74
12.To be able to set remote wipe out of files on the mobile phone	3.68	1.33
13.To be able to use the e-commerce securely	3.42	1.09
14.To be able to differentiate normal e-mails and spam mails	3.46	1.36
15To be able to setup owner details if the phone is stolen	3.71	1.07
16.To be able to delete all information on the phone before changing my phone	3.71	0.87
Average	**3.72**	**1.27**

5.2 Difference based on Gender towards Mobile Phone Security

In order to find whether there is any gender based difference in university students' self-efficacy towards mobile phones security or not an independent samples *t*-test was employed. According to the Table 5.2, concerning the self-efficacy and students' perception towards mobile phone security, there are statistically significant differences between male and female in this study ($p<.05$). The research results showed that male and female students have different security perception towards mobile phone security. The male students had higher mean values than female students.

Table 5.2: Gender based difference on mobile phone security amongst students

Gender	N	Mean	SD	Mean Difference	t	P
Male	249	4.114	.737	.734	10.977	.000*
Female	308	3.380	.821			

* $p<0.05$

Past examination on sexual orientation and innovation use proposes that contentions might effectively exist in how males and females utilize their mobile phones (Hakoama and Hakoyama, 2011; Haverila, 2011). Established on his review of sexual orientation designs in mobile phone use, Grover et al. (2011) reasons that, the inspirations and objectives of mobile phone use reflect rather ordinary sexual orientation parts. By et al. (2011) men see a more instrumental use for mobile phones though ladies use the mobile phone as a social tool. Gotten with landline telephones too, this utilization design among male and female phone clients speaks to a standout amongst the most strong examination discoveries to date as far as perceiving how distinctive thought processes produce extraordinary use designs over a differences of innovations (e.g., the Internet). Junco et al. (2013) found that female understudies sent more messages and talked longer on their mobile telephone sets that their male partners.

Females have a tendency to comprehend innovations like mobile telephone sets and the web as tools of correspondence - as a method for saving and managing connections. Men, then again, have a tendency to consider the Internet and related innovations as wellsprings of stimulation (Robert et al., 2014) and/or as wellsprings of information. In a subject taking a gander at

Facebook compulsion, Kuss and Griffiths (2011) reason that females, dissimilar to their male partners, have a tendency to use social networking sites to a great extent to speak with individuals from their associate group.

5.3 Difference based on Age towards Mobile Phone Security

In order to understand whether there is any age based difference in university students' self-efficacy towards mobile phones security? One-way ANOVA was employed. As indicated in Table 5.3, in this study there are statistically significant differences between all ages towards mobile phone security amongst students ($p<0.05$). Students in the Age group 18-19 had the highest mean value of 3.981±0.779, followed by age group of 22-25+ with mean value of 3.708±0.865, this might be due the fact more study between the age group of 18-19 and 22-25+ paid much attention to their mobile phone security and showed more interest in the ensuring safe use of their mobile phones, while students in the age group 20-21 had the lowest mean value of 3.421±0.907. This result suggests that students between the age group 18-19 pay more attention to mobile phone security than students in other age groups. This study was in agreement with that of Fowler and Noyes (2015) who reported from their study that university students from age 18 and over make good use of their mobile than older students.

From Table 5.4, there are significant differences ($p<0.05$) amongst students' opinions on mobile security in all age groups.

Table 5.3: Age based difference in mobile phone security amongst students

Age	N	Mean	SD	Mean Square	F	P
18-19	200	3.981	.779			
20-21	157	3.421	.907	14.124	20.205	.000*
22-25+	200	3.708	.865			

* $p<0.05$

An expanding dependence on mobile phones among youthful grown-ups and undergrads might flag the improvement of mobile phone use from a propensity to a fixation. In spite of the fact that the idea of fixation has various definitions, customarily it has been accounted for as the rehashed propensity for a substance in spite of the negative impacts endured by the

dependent individual (Alavi et al., 2012). All the more of late, the thought of enslavement has been summed up to incorporate practices such as betting, sex, occupation, eating, Internet, and mobile-telephone use (Roberts and Pirog, 2012). Any element that can make a pleasurable sensation has the capability of getting to be addictive (Alavi et al., 2012). Like substance compulsion, behavioral enslavement is best seen as a constant drive or fixation to keep focused rehash a conduct in spite of its negative effect on one's prosperity (Roberts and Pirog, 2012).

Table 5.4: Age based difference in mobile phone security amongst students multiple comparison

AGE	AGE	Mean Difference	Std. Error	95% Confidence Interval	
				Lower Bound	Upper Bound
18-19	20-21	.55984*	.09095	.3448	.7749
	22-25+	.31906*	.08066	.1286	.5095
20-21	18-19	-.55984*	.09095	-.7749	-.3448
	22-25+	-.24078*	.09334	-.4615	-.0201
22-25+	18-19	-.31906*	.08066	-.5095	-.1286
	20-21	.24078*	.09334	.0201	.4615

* $p<0.05$

5.4 Difference based on Mobile Operating System

In order to understand whether, there is any mobile operating system based difference in university students' self-efficacy towards mobile phone security, Mann-Whitney U test was carried out. According to the Table 5.5a, concerning the self-efficacy and students' perception towards mobile phone security, there are statistically significant differences between students using Android OS and Others OS in this study ($Z = -7.227$; $p = .000<.05$). The rank mean of the test of the Android OS group had a score mean rank of 309.94. The research results show that students using Android OS and Others OS have different security self-efficacy towards mobile phone security. The Android OS users had higher mean values than Others OS users.

Also looking at Table 5.5b, i.e., mobile phone operating system platform used by students other group frequency, iOS had the highest frequency of 42.95%, followed by Blackberry OS with value of 32.69% and the least value was Windows which is 24.36%.

Table 5.5a: Mobile phone operating system platform used by students

Mobile Platform	N	Mean Rank	Sum of Ranks	Mann-Whitney U	Z	p
Android	401	309.94	124284.00	18873.00	-7.227	.000*
Others	156	199.48	31119.00			

* $p<0.05$

Table 5.5b: Mobile phone operating system platform used by students other groups Frequency (N= 156)

Mobile Platform of Others	N	Frequency (%)
iOS	67	42.95
Blackberry OS	51	32.69
Windows	38	24.36

This outcome was in accordance with that of Bala et al. (2015) who reported that a lot of students use Android Operating System empowered mobile telephones than others Mobile phone working frameworks. By and Kale (2013) amid late years, the offer of advanced mobile phones in general handheld mobile specialized gadget deals has definitely expanded. Among them, the Android working framework by the Open Handset Alliance, noticeably drove by Google Inc., is business sector overwhelming. In Q3 2011, 52.5% of all gadgets sold were Android gadgets, trailed by Symbian (16.9%) and Apple's iOS (15.0%), as indicated by their

examination with the far reaching utilization of advanced mobile phones both in private and business related ranges, securing these gadgets have happened to principal significance. Proprietors utilize their advanced cells to do tasks extending from ordinary correspondence with loved ones to the administration of saving money accounts and getting to touchy business related data. These components, consolidated with constraints in managerial gadget control through proprietors and security basic applications like the Mobile TAN for keeping money exchanges, make Android based (Bagal and Kale, 2013).

5.5 Difference based on Mobile Phone Usage

In order to understand whether, there is any mobile phone usage based difference in university students' self-efficacy towards mobile phones security? Mann-Whitney U test was carried out. According to the Table 5.6, concerning the self-efficacy and students' perception towards mobile phone security, there are statistically significant differences between students using social media regularly and other purposes in this study ($Z = -3.308$; $p = .001<.05$). The rank mean of the test of the Android OS group had a score mean rank of 289.93.

Table 5.6: Mobile usage of mobile phone security amongst students

Mobile Usage	N	Mean Rank	Sum of Ranks	Mann-Whitney U	Z	p
Social Media	451	289.93	130758.50	18973.50	-3.308	.001*
Others	106	232.50	24644.50			

* $p<0.05$

The research results showed that students using social media regularly and other purposes have a different security self-efficacy towards mobile phone security. The students using social media regularly had higher mean values than other purposes. This result was in accord with that of Bacchus and Polichar (2010) whose report peruses that most students utilized their mobile telephone sets for calling, social media activities and sending of SMS. Thomee (2012) reported that most students use their mobile telephone sets for calling and for social media activities. North et al. (2014) Mobile phones are perceived to be truly famous among college

students, expanding their social inclusion and connectedness and in addition giving a suspicion that all is well and good as they can achieve others in times of trouble or crisis. Despite the fact that there are numerous advantages of using a mobile phone, there can likewise be negative consequences for the clients and nature. Addresses are upset when mobile phones are utilized at wrong times (Walsh et al., 2010), and utilizing a mobile phone whilst driving might prompt an expanded peril of a mishap (Hong et al., 2012; Walsh et al., 2010). Other negative impacts of mobile phone use incorporate enslavement, showed as over reliance, which can make inconveniences, for example, passionate anxiety, harmed connections, and falling proficiency (Balakrishnan and Raj, 2012). North et al. (2010) college students were accounted for to display indications of intellectual striking nature, whereby students consider their telephones when they are not using them, and in addition behavioral remarkable quality, whereby the students continually check their mobile phones for missed calls or messages. Chakraborty (2006) reported that most students in India use their mobile phone for social media activities. Krithika and Vasantha (2013) also reported from their study that most India students use their mobile phone for social media activities. And finally Ezemeenaka (2013) reported from his study that most students in Nigeria use their mobile phone for social media activities which invariably affect their academic performance due to high and intense concentration on their mobile phone.

CHAPTER 6
CONCLUSION AND RECOMMENDATIONS

6.1 Conclusion

In Libya all mobile phones, are potential targets of attacks which exploit the weaknesses related to mobile telephone sets that arise as a substance of communication like SMS, MMS, GSM, Wi-Fi networks, Bluetooth, or basic downloading from the net. There are attacks that exploit the software exposure to web browser and operating system. Lastly, there are varieties of malicious software that rely on the weak knowledge of ordinary users.

Mobile phones are being frequently used by students on a daily basis for various purposes, such as making of phone calls, browsing, chatting, downloading of application, etc. and this invariably makes their mobile and files most times completely unsecure. However ability for students to use their mobile phone safely will avert hacking if not totally but to a great height.

The results of this study give a good insight on the awareness of students towards mobile phone security. With the results of this study, it could be deducted that the results of this study will be of valuable help to the students, parents and most probably the government or universities of Libya to know the possible weakness of students' knowledge of mobile phone security issues and help propose a possible solution that will help salvage this problem.

6.2 Recommendations

With respect to this particular research, it is urged that there should be more awareness on mobile security to all strata of students depending on their staffs, and further work should be counted into this subject field. In spite of the restrictions, the present study ought to give the stimulus to new examinations to refine the comprehension of cellular telephone use amongst college understudies. Further research could examine other basic variables that make due inside of the biological communities of the understudies that could shape their cell telephone carries on. In summation, the outcomes of extraordinary cellular telephone use could be further investigated as far as level of mental indications seen by clients of the cellular telephone.

REFERENCES

AICPA, (2011). Top technology initiatives, American institute of certified public accountants. Retrieved, 10/22/2010 from http://www.aicpa.org/interestareas/informationtechnology/resources/toptechnologyinitiatives/pages/2010topteninitiatives-complete.aspx.

Alavi, S. S., Ferdosi, M., Jannatifard, F., Eslami, M., Alaghemandan, H., & Setare, M. (2012). Behavioral addiction versus substance addiction: Correspondence of psychiatric and psychological views. *International Journal of Preventive Medicine, 3*(4), 290–294

Alfawareh, H. M., & Jusoh, S. (2014). Smartphones usage among university students: Najran University case. *International Journal of Academic Research Part B, 6*(2), 321-326.

Alhussain, T., AlGhamdi, R, Alkhalaf, S., & Alfarraj, O. (2013). User's perceptions of mobile phone security: A Survey Study in the Kingdom of Saudi Arabia. *International Journal of Computer Theory and Engineering, 5*(5), 793-796.

Androulidakis, I., & Kandus, G. (2011). What university *students* do (or don't) know about security in their mobile phones. *Telfor Journal, 3*(1), 8-12.

Aoki, K., & Downes, E. J. (2010). An analysis of young people's use of and attitudes toward mobile phones. *Telematics and Informatics, 20* (4), 349-364.

Bagal, N.S., & Kale, N. D. (2013). Android open-source operating system for mobile devices. *IOSR Journal of Computer Engineering, 11*(5), 25-29.

Bala, K., Sharma, S., & Kaur, G. (2015). A study on smartphone based operating system. *International Journal of Computer Applications, 121*(1), 0975 – 8887.

Balakrishnan, V., & Raj, R. G. (2012). Exploring the relationship between urbanized Malaysian youth and their mobile phones: A quantitative approach. *Telematics and Informatics, 29*(3), 263–272.

Barkhuus, L., & Polichar, V. E. (2010). Empowerment through seamfulness: smart phones in everyday life. *Persons Ubiquitous Computing*, 1-11.

Baron, N., & Campbell, E. (2010). Talking takes too long: gender and cultural patterns in mobile telephony. *In Proceedings of the Conference of Association of Internet Researchers*. Göteborg, Sweden, *11*(2) 123-234.

Baron, N. S. (2010). Cross cultural patterns in mobile phone use: public space and reachability in Sweden, the US, and Japan. *New Media & Society, 12* (1), 13-34

Beaver, T., Knox, D., & Zusman, M. (2010). Hold the phone! mobile phone use and partner reaction among university students. *College Student Journal*, *44*(3), 629–632.

Becher, M., Freiling, F. C., Hoffmann, J., Holz, T., Uellenbeck, S., & Wolf, C. (2011). Mobile security catching up? Revealing the nuts and bolts of the security of mobile devices. *In Proc. 2011 IEEE Symposium on Security and Privacy*, *96*–111.

Bell, G., & Dourish, P. (2009). Yesterday's tomorrows: notes on ubiquitous computing's dominant vision. *Personal Ubiquitous Computing*, *11*(2), 133–143

Braguglia, K. H. (2010). Mobileular telephone use: a survey of college business students. *Journal of College Teaching & Learning*, *5*(4), 55-62.

Brown, A. (2011). Smartphone usage. Retrieved 23/11/2010, from http://www.compukiss.com/articles/smartphones-usage.html

Carlson, P. J., Kahn, B. K., & Rowe, F. (2010). Organizational impacts of new communication technology: A comparison of mobileular phone adoption in France and the United States. *Journal of Global Information Management*, *7*(3), 19- 29.

Castells, M., Mireia, F., Qiu, J., & Sey, A. (2010). The mobile communication society. research report for the international workshop on wireless communication policies and prospects: *A Global Perspective.* Retrieved 33/1/2010, from http://annenberg.usc.edu/international_communication/WirelessWorkshop/M CS.pdf

Cheng, J., Wong, S.H., Yang, H., & Lu, S. (2007). SmartSiren: virus detection and alert for smartphones. *In Proceedings of the 5th international Conference on Mobile Systems, Applications and Services.,23* 14-34.

Chen, Y.-F., & Katz, J. E. (2009). Extending family to school life: College students' use of the mobile phone. *International Journal of Human-Computer Studies*, *67*(2), 179–191.

Clarke, N., & Furnell, S. (2010). Advanced user authentication for mobile devices. *Computers and Security, 26*(2), 109-119.

Cooper, G. (2012). Who's watching whom? Monitoring and accountability in mobile relations. In B. Brown, N. Green, and R. Harper, (Eds.) Wireless world: social and interactional aspects of the mobile age. London: Springer.

CTIA Semi-Annual Wireless Industry Survey, (2010). Washington DC: CTIA-The Wireless Association. Retrieved 1/6/2010, from http://www.ctia.org/research_statistics/index.cfm/AID/10030

Dresler-Hawke, E., & Mansvelt, J. (2008). Mobile phones: Enhancing social communication in young adult's lives? *Presentation at the Australian and New Zeal and Marketing Academy Conference*. Sydney, Australia, 1–7.

Felt, A., Finifter, M., Chin, E., Hanna, S., & Wagner, D. (2011). A survey of mobile malware in the wild, *SPSM '11, Proceedings of the 1st ACM Workshop on Security and Privacy in Smartphones and Mobile Devices*, 2011, Chicago, Illinois, 3-13.

Fowler, J., & Noyes, J. (2014). Attitudes and use of mobile phones in tweens. *Advances in the Human Side of Service Engineering 1*, 40-51.

Fowler, J., & Noyes, J. (2015). From dialing to tapping: University students report on mobile phone use. *Procedia Manufacturing, 3,* 4716 – 4723.

Gartner Press Release (2010). Gartner says mobile phone sales will exceed one billion in 2009. Retrieved 23/1/2010, from http://www.gartner.com/press_releases/asset_132473_11.html

Gelenbe, E., Gorbil, G., Tzovaras, D., & Liebergeld, S. (2013). Security for Smart Mobile Networks: The NEMESYS Approach. *In: Proceeding of International Conference on Privacy and Security in Mobile Systems (PRISMS), IEEE*, 1-8.

Georgia Tech Information Security Center (2009), *Emerging Cyber Threats Report for 2009*. Retrieved 23/4/2009 from http://www.gtisc.gatech.edu/pdf/CyberThreatsReport2009.pdf

Geser, H. (2006). Preen teen smartphone adoption: consequences for later patterns of phone usage and involvement, Sociology of the Mobile Phone. Retrieved 30/1/2006 from http://socio.ch/mobile/t_geser2.html

Gohring, N. (2012). New Trojan horses threaten mobile phones, *PC World.* Retrieved 32/12/2012 from http://www.pcworld.com/article/124448/new_trojan_horses_threaten_mobile_phones.html.

Gregg, M. (2010). Predictions: What's the worst network security threat this year?, TechTarget.com, Retrieved, 3/7/2010 from http://searchnetworking.techtarget.com/generic/0,295582,sid7_gci1379874,00.html.

Grellhesl, M., & Punyanunt-Carter, N. M. (2012). Using the uses and gratifications theory to understand gratifications sought through text messaging practices of male and female undergraduate students. *Computers in Human Behavior, 28*(6), 2175–2181.

Grover, A., Kamins, M. A., Martin, I. M., Davis, S., Haws, K., Mirabito, A. M., Mukherjee, S., Pirouz, D., & Rapp, J. (2011). From use to abuse: When everyday consumption behaviors morph into addictive consumptive behaviors. *Journal of Research for Consumers,* 19, 1–8.

Hakoama, M., & Hakoyama, S. (2011). The impact of mobile phone use on social networking and development among college students. *The American Association of Behavioral and Social Sciences Journal*, *15*, 1–20.

Haverila, M. J. (2011). Mobile phone feature functions and gender differences among college students. *International Journal of Mobile Communications*, *9*(4), 401–419

Hofvenschiold, E. (2010). Determining cultural issues in attitude to and use of mobile phones. *In: Proceedings of the German Chapter of Usability Professionals*, 171-174.

Hong, F. Y., Chiu, S. I., & Huang, D. H. (2012). A model of the relationship between psychological characteristics, mobile phone addiction and use of mobile phones by Taiwanese university female students. *Computers in Human Behavior*, 28(6), 2152–2159.

Ingerman, B., Yang, C., & the 2011 EDUCAUSE Current Issues Committee (2011), Top-Ten It Issues, *EDUCAUSE Review*, (46), 12-28.

Issac, H., Nickerson, R., & Tarasewich, P. (2011). Mobile phone use in social settings: preliminary results from a study in the United States and France. *In: Proceedings of the Decision Science Institute Annual Meeting*. Retrieved 13/3/2011, from http://www.ccs.neu.edu/home/tarase/

Ito, M., Okabe, D., & Matsuda, M. (eds) (2008). Personal, portable, pedestrian: mobile phones in Japanese life. MIT Press, Cambridge.

Jackson, L. A., Von Eye, A., Fitzgerald, H. E., Zhao, Y., & Witt, E. A. (2010). Self-concept, self-esteem, gender, race and information technology use. *Computers in Human Behavior, 26*(3), 323–328.

Jiang, X (2011). Security Alert: New sophisticated android malware droid kungfu found in Alternative Chinese App Markets. Retrieved 25/1/2015 http://www.cs.ncsu.edu/faculty/jiang/DroidKungFu.html

Jones, B. H., & Heinrichs, L. R. (2012). Do business students practice smartphone security? *Journal of Computer Information Systems,* 22-30.

Junco, R., & Cotton, S. R. (2012). No A 4 U: The relationship between multitasking and academic performance. *Computers & Education, 59,* 505–514.

Junco, R. (2013). Comparing actual and self-reported measures of Facebook use. *Computers in Human Behavior, 29,* 626–231.

Karlson, A. K., Brush, A. B., Schechter, S. (2009). Can i borrow your phone?: Understanding concerns when sharing mobile phones. *In: Proceedings of Computer-Human Interaction*. ACM, New York, 1647–1650.

Kavur, J. (2009). Mobile trends and future technologies, *CIO*. Retrieved 21/2/2009 from http://www. cio.com/article/510076/20_Mobile_Trends_and_Future_Technologies.

Keizer, G., (2010). Gizmodo paid $5k for next-gen iphone, *Computer world*. Retrieved, 23/1/2010 from http://www.computerworld.com/s/article/9175819/Gizmodo_paid_5K_for_next_gen_iPhone.

Kim, J. L., & Altmann, J. (2013). Adapting smartphones as learning technology in a korean university. *Journal of Integrated Design and Process Science, 17*(1), 5-16

Kim, S. H., & Leem. C. S. (2010). Security threats and their countermeasures of mobile portable computing devices in ubiquitous computing environments. *In: Proceeding of International Conference on Computational Science and its Application, 3483,* 79 – 85.

Kindberg, T., Spasojevic, M., Fleck, R., & Sellen, A. (2009). I saw this and thought of you: some social uses of camera phones. *In: Proceedings of Computer-Human Interaction*. ACM, New York, 1545–1548.

Kruger, H. A., & Kearney, W. D. (2006). A prototype for assessing information security awareness. *Computer Security, 25* 289-96.

Kuss, D. J., & Griffiths, M. D. (2011). Excessive online social networking: can adolescents become addicted to Facebook? *Education and Health, 29*(4), 68–71.

Kuznekoff, J. H., & Titsworth, S. (2013). The impact of mobile phone usage on student learning. *Communication Education*, 62(3), 233-252.

Lawton, G. (2008). Is it finally time to worry about mobile malware? *Computer*, *41*(5), 12-14.

Lee, S.Y. (2014). Examining the factors that influence early adopters' smartphone adoption: The case of college students. *Telemat. Inf.*, 31(2), 308-318.

Lenhart, A. (2012). Teens, Smartphones and Texting. Pew Research Center's Internet & American Life Project, 1-34. Retrived from http://pewinternet.org/Reports/2012/Teens-and-smartphones.aspx

Ling, R., & Yttri, B. (2002). *Hyper-coordination via mobile phones in Norway*. In Katz, J. E., & Aakhus, M. (Eds.), Perpetual Contact: Mobile Communication, Private Talk, Public Performance. Cambridge: Cambridge University Press. 2002.

Ling, R. (2004). The mobile connection: the mobile phone's impact on society. Morgan Kaufmann, Boston. *In: Proceedings of Computer-Supported Cooperative Work*, ACM, NY, 21–25.

Ling, R., & Horst, H. (2011). Mobile communication in the global south. *New Media & Society*, 13(3), 363–374

Lobo, D., & Joshma, P. J. (2013). A study to assess the impact of mobile phone use on various dimensions of students' life in a selected institution of Mangalore. *International Journal of Nursing Education*, 5(2), 62-65.

Lomo-David, E., & Shannon, L. (2010). Information systems security and safety measures: the dichotomy between students' familiarity and practice. *Academy of Information and Management Sciences Journal*, 12(1), 29-47.

Madell D., & Muncer, S. J. (2004). Back from the beach but hanging on the telephone? English adolescents attitudes and experiences of mobile phones and the Internet, *Cyber psychology & Behaviour, 7*(3), 359-367

Maslennikov. D. (2011). ZeuS-in-the-Mobile is back, *securelist blog*. Retrieved 23/1/2011, fromhttp://www.securelist.com/en/blog/11169/Zeus_in_the_Mobile_is_back.

Mazmanian, M., Yates, J., & Orlikowski, W. (2009). Ubiquitous email: individual experiences and organizational consequences of Blackberry use. *In: Proceedings of the 65th annual meeting of the academy of management*. Atlanta, GA.

McGuigan, J. (2012). Towards a sociology of the mobile phone. *Human Technology*, 1(1), 12-17.

Meeker, M., Devitt, S., and Wu, L. (2010). *Internet Trends,* a Morgan Stanley report, Retrieved 23/1/2010 from http://www.morganstanley.com/institutional/techresearch/internet_trends042010.html.

Mehrotra, A., & Nguyen, A. (2012). Differences in phone use between men and women: Quantitative evidence from Rwanda. *In Proceedings of the Fifth International Conference on Information and Communication Technologies and Development* (297–306). California: ACM.

Mensch, S., & Wilkie, L. (2011). Information security activities of college students: an exploratory study. *Academy of Information and Management Sciences Journal*, 14(2), 91-116.

Middleton, C., & Cukier, W. (2009). Is mobile email functional or dysfunctional? Two perspectives on mobile email usage. *European Journal Information System 15*(3):252–260.

Mohtar, N.M. M., Hassan, M. A., Hassan, M. S. & Osman, M. N. (2013). The importance of smartphone's usage among Malaysian undergraduates. *IOSR Journal of Humanities and Social Science*, *14*(3), 12-118.

Motorola, (2010). Towards the next billion subscribers: Motorola delivers on seamless mobility vision. Retrieved, 23/2/2010 from http://www.motorola.com/mediacenter/news/detail/0,,6405_6355_23,00.html#f n1

North, D., Johnston, K., & Ophoff, J. (2014). The use of mobile phones by South African university students. *Issues in Informing Science and Information Technology*, 11, 115-138.

Nylander, S., Lundquist, T., & Brannstrom, A. (2009). At home and with computer access: why and where people use mobile phones to access the internet. *In: Proceedings of Computer-Human Interaction*. ACM Press, New York, 1639–1642.

Ofcom Facts & Figures, 2014. Retrieved 22/1/2014, from http://media.ofcom.org.uk/facts/

O'Hara, K., Mitchell, A. S., Vorbau, A. (2009). Consuming video on mobile devices. *In: Proceedings of Computer-Human Interaction.* ACM, New York, 857–866.

Ogunyemi, O. (2010). Consumption and (in) appropriate use of mobile phone among teenage Africans in the UK. Lincolnshire, England.

Palen, L., Salzman, M., & Youngs, E. (2009). Going wireless: behavior & practice of new mobile users. *In: Proceedings of Computer-Supported Cooperative Work,* ACM, NY, 201–210.

Palen, L., Salzman, M., & Youngs, E., (2010). Going wireless: behavior & practice of new mobile phone users. *In: Proceedings of the conference on Computer supported cooperative work,* 11-22.

Panko, R. (2010). *Business data networks and telecommunications,* 7th Edition, Pearson Prentice Hall.

Park, N., & Lee, H. (2012). Social implications of smartphone use: Korean college students' smartphone use and psychological well-being. *Cyber Psychology, Behavior & Social Networking, 15*(9), 491-497.

Payne, K. B., Wharrad, H., & Watts, K. (2012). Smartphone and medical related App use among medical students and junior doctors in the United Kingdom (UK): a regional survey. *BMC Medical Informatics Decision Making,* 12, 1-11.

Rao, L. (2012). comScore: 4 Out Of 5 Smartphone owners use device to shop; amazon is the most popular mobile retailer. *Tech Crunch*. AOL Inc.

Roberts, J. A., & Pirog, S. F. (2012). A preliminary investigation of materialism and impulsiveness as predictors of technological addictions among young adults. *Journal of Behavioral Addictions, 2*(1), 56–62.

Roberts, J. A., Yaya, L. H. P., & Manolis, C. (2014). The invisible addiction: Mobile-phone activities and addiction among male and female college students. *Journal of Behavioral Addictions, 3*(4), 254–265.

Scott, M., Acton, T., & Hughes, M. (2010). An assessment of biometric identities as a standard for e-government services. *Services and Standards, 1*(3), 271-286.

Sharma, T.N., Beniwal, M. K., & Sharma, A. (2013). Comparative study of different mobile operating systems. *International Journal of Advancements in Research & Technology, 2*(3), 1-5.

Shropshire, J., Warkentin, M., & Johnston, A. (2010). Impact of negative message framing on security adoption. *Journal of Computer Information Systems*, 51(1), 41-51.

Sipahi, B., Yurtkoru, E.S., & Cinko, M. (2010). Sosyal bilimlerde spss'le very analizi. Istanbul: Beta Yaninlari.

Smith, A. (2011). Americans and their mobile phones. A report from the Pew Internet and American Life Project, Retrieved, 23/4/2011, from http://www.pewinternet.org/Reports/2011/Mobile-Phones.aspx?src=prc-headline.

Sohn, T., Li, K. A., Griswold, W. G., & Hollan, J. D. (2008). A diary study of mobile information needs. *In: Proceeding of Computer-Human Interaction.* ACM, New York, 433–442

Suominen, A., Hyrynsalmi, S., & Knuutila, T. (2014). Young mobile users: Radical and individual – Not. *Telematics and Informatics*, 31(2), 266-281.

Talib S, Clarke N, & Furnell S. (2010). An analysis of information security awareness within home and work environments. *In: Proceedings of international conference on Availability, Reliability and Security (ARES)*, Krakow, Poland; 196-203.

Teer, F., Kruck, S., & Kruck, G. (2010). Empirical study of students' computer security practices/perceptions. *Journal of Computer Information Systems*, 105-110.

Thomee, S. (2012). ICT use and mental health in young adults Effects of computer and mobile phone use on stress, sleep disturbances, and symptoms of depression. Master's Thesis in Occupational and Environmental Medicine Department of Public Health and Community Medicine Institute of Medicine at Sahlgrenska Academy University of Gothenburg, 1-88.

Townsend, A.M. (2010). Mobile communications in the twenty-first century city. In B. Brown, N. Green and R. Harper (eds.), Wireless World: Social and Interactional Aspects of the Mobile Age, 62-77, Springer.

Tsohou A, Karyda M, Kokolakis S., & Kiountouzis E. (2012). Analyzing trajectories of information security awareness. *Information Technology, 25*(3):327-52

Uys, W. Mia, A., Jansen, G. J., Schyff, H.V., Josias, M. A., Khusu, M., Gierdien, M., Luekes, N. A., Faltein, S., Gihwala, T., Theunissen, T., & Samsodie, Y. (2012) Smartphone

Application Usage Amongst Students at a South African University. *In: proceedings of IST-Africa Conference*, 1-11.

Venkatesh, A. (2010). Ethnoconsumerism: A new paradigm to study cultural and cross-cultural consumer behavior. In J.A. Costa and G. Bamossy (eds.), Marketing in the Multicultural World, SAGE Publications, 26-67.

Wahlisch, M., Vorbach, A., Keil, C., Schonfelder, J., Schmidt, T. C., & Schiller, J. H. (2013). Design, implementation, and operation of a mobile honeypot. *arXiv Computing Research Repository*, 130-137.

Walsh, S., White, K., & Young, R. (2010). Needing to connect: the effect of self and others on young people's involvement with their mobile phones. *Australian Journal of Psychology*, 62(4), 194–203.

Wei, F.-Y. F., Wang, Y. K., & Klausner, M. (2012). Rethinking college students' self-regulation and sustained attention: Does text messaging during class influence cognitive learning? *Communication Education*, 61, 185-204.

Weilenmann, A., & Larsson, C. (2010). Local use and sharing of mobile phones. In B. Brown, N. Green & R. Harper (Editors.) Wireless World: Social and Interactional Aspects of the Mobile Age. *Godalming and Hiedleburg: Springer Verlag*, 99-115

Whitney, L. (2010). Smartphones to Dominate PCs in Gartner Forecast, CNET Business Tech News. Retrieved, 23/1/2010 from http://news.cnet.com/8301- 1001_3-10434760-92.html?tag=mncol.

Wilksa, T. A. (2008). Mobile phone use as part of young people's consumption styles. *J Consum Policy*, *26*(4), 441–463.

World Fact Book 2012. Central Intelligence Agency. [Online]. Available: https://www.cia.gov/index.html.

Yan, G., & Eidenbenz, S. (2006). Bluetooth worms: models, dynamics, and defense implications. *In: Proceeding 22nd Ann. Computer Security Applications Conf.* (ACSAC 06), IEEE CS Press, 245-256.

Ying, L., Dinglong, H., Haiyi, Z., & Rau, P. (2010). Users' perception of mobile information security. *Information Security Technical Report*, 12, 162-171

Zahidi, F., & Hajj, W. E. (2009). Two factor authentication using mobile phones. *In Proceeding The 7th ACS/IEEE International Conference on Computer Systems and Applications (AICCSA-2009)*, Rabat, Morocco, 21-27.

Zhou, Y., & Jiang, X. (2012). Dissecting android malware: characterization and evolution. *In Proc. IEEE Symposium. on Security and Privacy,* 95–109.

Zulkefly, S. N., & Baharudin, R. (2010). Mobile phone use amongst students in a university in Malaysia: Its Correlates and Relationship to Psychological Health. *European Journal of Scientific Research, 37*(2), 206-218.

Ezemenaka, E. (2013). The usage and impact of Internet enabled phones on academic concentration among students of tertiary institutions: A study at the University of Ibadan, Nigeria. *International Journal of Education and Development using Information and Communication Technology, 9*(3), 162-173.

Krithika, M., & Vasantha, S. (2013). The mobile phone usage among teens and young adults impact of invading technology. *International Journal of Innovative Research in Science, Engineering and Technology, 2*(12), 7259-7265.

Chakraborty, S. (2006). Mobile phone usage patterns amongst university students: A comparative study between India and USA. A Master's Paper for the M.S. in I.S degree. April, 2006. 53 pages. Advisor: Diane Kelly. 1-55.

APPENDIX

SELF-EFFICACY AND PERCEPTIONS OF UNIVERSITY STUDENTS TOWORDS MOBILE PHONE SECURITY

The questionnaire aim to define your understand and opinions on mobile phone security. You are kindly expected to choose the best answer that you feel is closet to. The result of this questionnaire will solely be used for the analysis in the research report, and will not be provided to any institution in any way.

Thanks in advance for taking time to answer our questionnaire.

Assoc. Prof. Dr. Nadire Cavus
Khaled Adweb(Master Student)

SECTION 1: Personal Information (please tick the box most appropriate for you)

1. Gender □Male □Female

2. Age □ 18 - 19 □20-21 □22-25+

3. University name …….

4. Faculty……

5. Department……..

6. How many hours per day do you spend using mobile phone?
□Less than one hour □One hour
□Two hour □More than 2 hours

9. Mobile Platform
□Android □IOS □Blackberry OS □Windows

10. Regular purpose of using mobile phone
□Social media □Others

11. Do you use an antivirus on mobile phone?

□Yes □No

SECTION III: Scale for Self-Efficacy of University Students towards Mobile Phone Security (please tick the most appropriate to you)

Items		**Very Confident**	**Confident**	**Neutral**	**Not Confident**	**Not Very Confident**
1	To be able to know when a message containing a virus is received					
2	To be able to create a strong password for starting to use the mobile phone					
3	To be able to know how to password protect my mobile phone					
4	To be able to install latest security updates					
5	To be able to set auto-lock timer on mobile phone					
6	To be able to report stolen or lost mobile phone with owner details					
7	To be able to change the password from time to time					
8	To be able to disable wireless access such as Bluetooth and WIFI when not required					
9	To be able to password protect secure data stored on the phone					
10	To be able to logout when the device is not in use					
11	To be able to set encryption on personal and important files					
12	To be able to set remote wipe out of files on the mobile phone					
13	To be able to use the e-commerce securely					
14	To be able to differentiate normal e-mails and spam mails					

15	To be able to setup owner details if the phone is stolen					
16	To be able to delete all information on the phone before changing my phone					