THE AWARENESS OF PARENTS TOWARDS THE SAFE USE OF THE INTERNET

A THESIS SUBMITTED TO THE GRADUATE SCHOOL OF APPLIED SCIENCES

OF

NEAR EAST UNIVERSITY

By

KHAIRI GHET ELGHADAFI ELGHARNAH

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

NICOSIA, 2020

KHAIRI GHET
ELGHARNAH

THE AWARENESS OF PARENTS TOWARDS
THE SAFE USE OF THE INTERNET

NEU
2020

THE AWARENESS OF PARENTS TOWARDS THE SAFE USE OF THE INTERNET

A THESIS SUBMITTED TO THE GRADUATE SCHOOL OF APPLIED SCIENCES

OF

NEAR EAST UNIVERSITY

By

KHAIRI GHET ELGHADAFI ELGHARNAH

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

NICOSIA, 2020

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:

Signature:

Date:

ACKNOWLEDGEMENTS

First of all, I would like to introduce my thankfulness and appreciation to my supervisor Prof. Dr. Fezile Özdamli for her supervision on my thesis, she was friendly and respectful during the time we spend on the thesis, she helped and guided me in each stage of the research especially with those difficult things throughout the thesis until we reached to finish the writing steps and forms of the thesis research.

I would like to be thanks and gratitude to my family, my parents, my brothers, and sisters, and my wife for their feeling of love to me and encouragement during my study in North Republic Cyprus.

As well I would like to say thanks to all my friends for their encouraged and supported in my studying.

Finally, I would be grateful to everybody who contributes with me during my study and complete my thesis work, Near East University staff, colleagues, and parents who participants in this study.

To my parents…

ABSTRACT

Internet security safety awareness of parents is an important issue that should be addressed to raise the knowledge and awareness level about internet risks, information privacy, safety concerns and online attacks among parents so that they will be able to teach their children how to use the internet safety. The internet technology has brought many benefits for children such as solving their difficult homework online, learning new skills, communicating and sharing information with other children and their teachers. Despite the great importance of the internet, they have been reports of it is users falling victims to cybercrime attacks by losing their private information to such password and pin number to attackers. Also, children are exposed to pornography content and other violent content which might have a negative impact on their behavior and thinking. This study investigates the awareness of parents towards the safe use of the internet. A questionnaire sample was distributed containing questions on the characteristics of internet security and safety. A total of 252 participants who their children study at Near East University schools (Near East Libyan school) were targeted in this study. Data were collected and analyzed by using SPSS software. According to the results, it was confirmed that there is no statistically significant difference between relative relationship variables and all dimensions of the questionnaire.

Keywords: Internet security safety; parents awareness; children; internet risks; information privacy

ÖZET

Ebeveynlerin İnternet güvenliği ve emniyeti bilinci, çocuklarına İnternetin nasıl güvenli bir biçimde kullanılacağını öğretebilmeleri, İnternet ile ilişkili riskler, bilgi gizliliği, güvenlik endişeleri ve çevrimiçi saldırılar hakkında bilgi ve farkındalık düzeyini yükseltmek için ele alınması gereken önemli bir konudur. İnternet teknolojisi, çocuklar için zor olan ev ödevlerini çevrimiçi olarak çözebilme, yeni beceriler öğrenme, diğer çocuklarla ve öğretmenleriyle iletişim kurma ve bilgi paylaşma gibi birçok fayda sağlamıştır. İnternetin büyük önemine ragmen, siber suç saldırılarına kurban düşen kullanıcıların, şifre ve pin numarası gibi gizli bilgilerinin saldırganlar tarafından ele geçirildiği rapor edilmiştir. Ayrıca, çocuklar pornografi içeriğine ve davranışları ve düşüncelerinde olumsuz etki oluşturabilecek diğer şiddet içeriklerine maruz kalmaktadırlar. Bu çalışma, ebeveynlerin İnternet'in güvenli kullanımına yönelik farkındalıklarını ve algılarını araştırmaktadır. İnternet güvenliği ve emniyetinin özellikleri hakkında sorular içeren bir anket örneği dağıtılmıştır. Bu çalışmada, çocukları Yakın Doğu Üniversitesi okullarında (Yakın Doğu Libya Okulu) okuyan 252 katılımcı hedeflenmiştir. Veriler SPSS yazılımı kullanılarak toplanmış ve analiz edilmiştir. Sonuçlara göre, göreceli ilişki değişkenleri ile anketin tüm boyutları arasında istatistiksel olarak anlamlı bir fark olmadığı doğrulanmıştır.

Anahtar Kelimeler: İnternet güvenliği emniyeti; ebeveynlerin farkındalığı; çocuklar; İnternet riskleri; bilgi gizliliği

TABLE OF CONTENTS

ACKNOWLEDGEMENTS ………………………………………………………..…….. ii

ABSTRACT ……………………………………………..……..……………… iv

ÖZET ……………………………………………………………….……..………….…. v

TABLE OF CONTENTS ……………………….………………..……….……... vi

LIST OF TABLES …………………………….……….…..………………… ix

LIST OF FIGURES ……………………………….……..………………… x

CHAPTER 1: INTRODUCTION

1.1 Background of the Study …………………………..……………....………….. 1

1.2 The Problem of the Study ……….. ……………………. ……….…………….. 3

1.3 The Aim of the Study ………………………………. ……………………..…... 5

1.4 The Significance of the Study ………………………………….……………… 5

1.5 Limitations of the Study ……………………………………….………………. 6

1.6 Overview of the Thesis ……………..……………………………..……………… 6

CHAPTER 2: RELATED RESEARCH AND THEORETICAL FRAMWORK

2.1 Related Research …………………………………….………………….……….... 7

2.1.1 Essential measures of online security ……………….……………….……….... 7

2.1.2 Protect information privacy on websites ……………….…………..…..… 8

2.1.3 Perceptions of parents to use the internet …….…………..…..…............. 10

2.1.4 The reliability of computer security software ……………...…………..….. 11

2.1.5 Self-efficacy for the safe use of the internet ……………..…………...….. 13

2.2 Theoretical Framework ……………………………………………………. 14

2.2.1 Perceptions of parents towards the safe use of the internet ………………… 14

2.2.2 Privacy security ……………………………………………….……..……... 15

2.2.3 Information privacy concerns ………………..……………………… 16

2.2.4 Internet security threats ……………. …..…….…………………..……..... 18

2.2.5 Online safety tips for parents to educate children to be safe use on the internet ………………………………………………………..… 21

CHAPTER 3: RESEARCH METHODOLOGY

3.1 Research Model of the Study…………...………..………..……….…….. 26

3.2 Research Participants ……. …………..………………………….……………..….. 27

3.3 Data Collection Tools ……………………………………………….……..……… 28

3.4 Reliability Test of Survey Dimensions …………….…….………………….………. 30

3.5 Research Procedure of the Study …….…….……………………...…………… 30

CHAPTER 4: RESULTS AND DISCUSSION

4.1 The Knowledge of Parents About Their Children's Internet Use ..……...…..…… 33

4.2 Parents' Use of Internet Connection Access Types ………………..…………… 34

4.3 Devices Used of Parents to Get Online ,………………..………………………. 34

4.4 The Awareness of Parents Towards the Safe Use of the Internet ………..……….. 35

4.5 The Differences Between Parents' Awareness Towards the Safe Use of the Internet Based on Relative Relationship Difference …………………...………… 38

4.6 The Differences Between Parents' Awareness Towards the Safe Use of the Internet Based on Age Groups Difference …………….…………………...…… 39

4.7 The Differences Between Parents' Awareness Towards the Safe Use of the Internet Based on Education level Difference ……………………………………. 40

CHAPTER 5: CONCLUSION AND RECOMMENDATIONS

5.1 Conclusion ………………………...…………………………………..……... 41

5.2 Recommendations ……………………………....…………………………… 42

REFERENCES ……………………….…..…………………………………………….. 43

APPENDICES……………………….…………..…………………….....……….……. 47

APPENDIX 1: Questionnaire ……………….…………………………..…...…… 48

APPENDIX 2: Ethical Approval Letter……….…..…....………………...…………… 53

APPENDIX 3: Similarity Report ……….…..…..……………………………………... 54

LIST OF TABLES

Table 3.1: Demographic information of participants ……………………...……… 28

Table 3.2: Cronbach's Alpha for the questionnaire factors ………………………... 30

Table 3.3: Time schedule of the research ……………………………..………… 31

Table 4.1: The knowledge of parents about their children's internet use ..……..……. 33

Table 4.2: Parents' internet connection access types……………….…………..…. 34

Table 4.3: The devices used of parents to get online…………………………...…... 34

Table 4.4: Explains the awareness of parents towards the safe use of the internet…… 35

Table 4.5: The total mean scores of each factor…………………………..……….. 38

Table 4.6: The differences between parents' awareness towards the safe use of the internet based on relative relationship difference……….……..………. 38

Table 4.7: The differences between parents' awareness towards the safe use of the internet based on age groups difference…..…………………..…..…… 39

Table 4.8: The differences between parents' awareness towards the safe use of the internet based on education level difference……………………..……. 40

LIST OF FIGURES

Figure 3.1: Research model of the study ……………………………….…………..… 27

Figure 3.2: The structure of the questionnaire ………………………..…………….. 29

Figure 3.3: Gantt chart of the study ………………………………………………… 32

CHAPTER 1

INTRODUCTION

This chapter presents an overview of the awareness of parents towards the safe use of the internet. It contains the background of the study, the problem, the aim, the significance as well as the limitations of this study.

1.1 Background of the Study

The awareness of parents about the safe use of the internet has become an important issue for online security. The risks associated with the internet as well as the security of personal information of the internet users is an issue of great concerns. The awareness and knowledge about internet safety will help parents to realize and to avoid undesirable online activates such as cybercrime, malicious software, and hacking which can enable unauthorized persons to have access to sensitive information. The study aims at creating awareness among parents on the need to educate their children on online safety and monitoring kids' activities such as the sites they visit, the people they meet on social media and the personal information they share with them. In recent years, the internet technology revolution has brought many advantages of online communication such as transferring information, sharing videos, files, online learning and chatting between users around the world. Furthermore, data are saved online at cloud computing companies which allow users to access their information where ever they are. However, internet security is a big issue for many people who have concern about their personal information privacy. According to Lee Hadlington et al. (2019), there are two kinds of critical components of information security; awareness represented in understanding organizational information security policy of users, and how users are able to implement the essentials of information security that has been organized.

Regarding Bada et al. (2014), internet information technologies have a large-scale use over the world and people's daily lives. For that, information security is of extreme significance. To obtain it, they post practical security measures and improve security policies that calm down the right behavior of internet users and people. A lot of users take these security issues for granted. This may be due to users' unconsciousness or adequate luck of awareness of the dangers involved and pour knowledge of the correct behavior in the use of the internet. The essential aim of online security awareness campaigns is to affect the adoption of online behavior security and to successfully teach users what they should do online for safe surfing online. The purpose of knowledge and security awareness of online risks are not for training but to focus on information security. Consciousness programs have the intention to let people realize information technology security concerns and react with it, which obviously should focus assurance on awareness. Persuasion techniques are how we can change behaviors or attitudes instead of using compulsion or cheating manner. To impact behavior, firstly by affecting what people consciously believe about intellectual or cognitive example, and secondly by molding behavior concentrated on the additional auto procedure of ruling and affect context template instead of altering the thinking. There are various components that should be taken to consider for an awareness campaign to be successful, one of them is that teaching new competencies effectively can drive to the prevention of high danger behavior over the internet.

In these modern days, people spend a lot of money to buy security technology to protect their data and computer systems against online attacks, some of the unlicensed computer security software contains malware programs which made to gain sensitive information of victims. Hardware and software security techniques used to make strong information systems against attacks. But this kind of security methods still exposed the attacks because of undesirable behaviors of internet users that are related to information security awareness (Öğütçü et al., 2016). Moreover, parents should learn how to be aware of the differences between legitimate emails and harmful emails. On the other hand, there are a variety of technologies for internet security that people can utilize to protect themselves from illegitimate access to the computer system or internet websites such as firewalls, Antivirus, user authentication, data encryption, virus detection, digital certificates, intrusion detection systems. Firewall protection represented in hardware or software used to control inbound and outbound on the local network to the internet. The firewall system is able to monitor and control the computer traffic over the internet through a variety of network packets to application protocols packets to determine firewall access policy to define security management and risk on the computer system (Grammatikis et al., 2019).

The research will be focused on the awareness of parents towards the safe use of the internet in order to be able to establish the policies and procedures that are necessary to protect the privacy and confidential data and to cover the deficiency awareness among parents about online security vulnerabilities. In addition, the study will help to fill the gaps in knowledge and awareness about online safety and security risky in order to keep parents and their children in a good security awareness by educating parents to be aware of online safety tips, privacy safety practice, social networking security, and good cyber ethics in order to avoid any unexpected accidents on the internet. The research consisted of a survey with a questionnaire sample to be completed by parents and the samples will be given to the children at Near East Libyan school in the Northern Republic of Cyprus. This study will educate and give online safety tips to the parents to be aware of keeping online safe use while they are surfing the internet and as well for purpose of being able to teach their children to be careful and keen on the awareness of internet safety. Parents should learn and be conscious of online privacy information on websites, and how to make strong passwords for their accounts and emails on websites, they should organize the time that they spend online to educate their kids and listen to children's online problems. Parent should know about controlling their laptops computers and install a good antivirus software and programs that can be blocked the undesirable websites (Kang, 2018; Benson, 2019; Schleicher, 2019).

1.2 The Problem of the Study

The internet connection is everywhere in the world, which leads to raising the size of online information that is used among users. This has increased the risk of internet security threats that affects the internet network, information security privacy, and computer systems. The increasing development of internet technology and accessibility to online information resources and communication with people around the world has led to arise the number of children participating in online communications. Thus, the possibility of exposing children to see a different unsuitable content such as pornographic materials, sexual, violent and exploitation is very high. Every day, the advertisements media, social networking, magazines, newspapers are full up of victims of cyber security threats and online cybercrime attacks. Hackers and cybercriminals developed and used many diverse techniques to attack privacy information and computer systems hacking, for instance, computer viruses, trojan, adware and spyware, computer worm, DOS and DDOS attack, phishing, internet fraud, hacking, ransomware, spam, malware, pharming, identity theft. Millions of computers have been attacked by one of these methods and millions of people have lost their data and their private information online, thousands of passwords have been stolen by hacking. In addition, many computer systems have been infected by DOS and distributed denial-of-service attacks in order to pay ransomware to hackers. Furthermore, a considerable number of bank accounts and credit cards that are processed online have attacked and customers lost sensitive data details. There are security concerns about devices connected with the internet of things, for example, wireless networks such as Bluetooth and Wi-Fi, and smart devices, including smartphones, televisions and the various tiny devices that constitute the internet of things are exposed to be attacked because of weak points of internet security of internet of things. The other vulnerabilities of internet security are the platforms of malicious software attacks represent in common free programs, inefficient antivirus, and file sharing such as BitTorrent.

Privacy worries mention the anxiety that people have with data privacy exercises of institutions, which could settlement the people's capability to monitoring personal data. E-business corporations utilize the personal information gathered by data observation, it is not only for adapting their products and services to a particular client demands however as well to grow their proceeds by selling declarations extent on their online sites. Even though the customized services and aimed to declare may interest assured customers, numerous customers have a concern about their information privacy that is not completely preserved. The sensation that they should have permission to monitor their personal data, also to be aware of what information is detected to other individuals. Information privacy of individuals are attacked via data exposure to third parties, or through other usages of personal information privacy without the person's approval. In this phase, the internet customers' worries about information privacy are a possible barrier to the success of e-business (Yun et al., 2019).

Personal privacy information on social media and websites is one of the big issues that threats people's privacy on social media such as Facebook, Instagram, and Twitter where people can share files, pictures, videos, chats, and other online activities. Facebook social networking presents privacy settings feature for their users to set and control the personal information, and activities online, however, many facebook users are not conscious of that privacy settings and they frequently leave privacy information remaining unprotected which exposes to online risks to be an essential goal for hackers to attack users' personal information (Gogus and Saygin, 2019). In 2018, Facebook has shared about 87 million of personal information of their users with Cambridge Analytica company without Facebook customers' assent (Yun et al., 2019). The essential motivation of this study is the increasing number of victims of online cybercrime and developing many different kinds of attack techniques used to attack the internet users' privacy by hackers. In addition, the awareness level and knowledge of internet security risks among internet users are very weak, especially among small age categories such as school children. This research intends to investigate the awareness of parents towards the safe use of the internet.

1.3 The Aim of the Study

The basic aim of the study is to explore the awareness of parents towards the safe use of the internet among parents, about internet security to raise the level awareness of parents and their children about internet security threats while they are surfing online. There are some questions around the research that the study will discuss in the results section in order to investigate the aim of this study.

1. Do parents have knowledge about their children' internet use?
2. Which devices do parents use to get online?
3. How is parents' awareness towards online security use?
4. What is the difference between parents' awareness towards the secure surfing online based on relative relationship?
5. Is there any difference between parents' awareness towards the secure use over the internet based on age?
6. Is there any difference between parents' awareness towards online safety use based on education level?

1.4 The Significance of the Study

According to internet security threats and the attacks on data privacy that happens every day online, many internet users are anxious about their information privacy which has become a controversial issue in our communities. Consequently, the study is very important to disseminate the importance of awareness of parents towards safe surfing over online among parents in order to be able to be aware of how to teach children to be careful of what they do online and have the adequate knowledge of the internet security issues represented in software malicious and cybercrime over the internet.

1.5 Limitations of the Study

This study will be limited to apply at Near East University schools only for determining and defining the importance of awareness level about the safe use of internet among parents in order to be aware of the internet risks and security threats such as DDoS, Phishing, cybercrime, etc.

1.6 Overview of the Thesis

The research was divided into five chapters in order to cover all data and results related to the study.

Chapter 1 has given an introduction to the awareness of parents towards the safe use of the internet, the problem of the study, the aim of the study, the significance of the study, the limitation and the scope of the study.

Chapter 2 presents background material concerning the study and related work.

Chapter 3 presents a detailed description of the methodology, data collection procedure, data analysis techniques, and statistical analysis of the research.

Chapter 4 presents the results and discussion, gives a description and interpretation of the study.

Chapter 5 presents the conclusions and recommendations of the study.

CHAPTER 2

RELATED RESEARCH AND THEORETICAL FRAMWORK

This part of the study will concentrate on the previous studies that are related to research about the awareness of parents towards the safe use of the internet. This research is based on the theoretical framework of this study.

2.1 Related Research

2.1.1 Essential measures of online security

According to privacy sensitivity use as a basic Westin's privacy index (Taylor, 2003) presented that privacy was not a matter for 9% of the sample. The individuals appeared hesitant when it approaches to expose private information while they reflected on the benefits of information exposure to far outbalance any prospect dangers. 41% of the sample can be assigned to the pragmatists' group. They scaled the prospect costs and benefits of information exposure before progressing. Pragmatists are willing to discover information if they realize their privacy protection assumptions met and the side in question to be authoritative. Fundamentalists are at a high level of privacy anxiety. They place liability for privacy protection at the individuals' level and request the proactive denial of information exposure by users.

Regarding the results of security issues and user privacy disclosed that the important concerns of participants are concentrated when users use their smartphones. Mostly, participants are anxious that mobile applications observe activities on phones which are collected users' personal information. The privacy attacks were increased relatively by mobile applications, which lead to raise the level of concerns of secondary use of personal information (Barth et al., 2019).

Security challenges in confidentiality, integrity, and availability may make a large effect loss in the business of cloud computing because the information is the main element for any business. Data integrity is the confirmation specified to the digital information that is allowed to be accessed only for authorized users. consequently, integrity includes preserving the accuracy, consistency, and trustfulness of data through the full life cycle. Maintaining confidentiality, integrity, and availability is easy in the establishment of computing. However, in cloud computing, it is more convoluted as the multi renter architecture and the distributed nature of the infrastructure (Kumar et al., 2018).

According to Schaik et al. (2018) online security in social networks, that Saridakis, Benson, Ezingeard, and Tennakoon (2016) have noted instability in the behavioral study on online social media, with numerous researches on information privacy, but there are a few types of researches on security issues. They studied about using social networks and security perceptions regarding online deception. As the results displayed that users with a high level of realizing dominant over personal information on social media, users who have rise conscious risk tendency on social networks and users of multi-objective social media are low probable to be victims of cybercrime. However, users of knowledge and awareness exchange social media are more probable to be victims.

2.1.2 Protect information privacy on websites

Information privacy awareness is the ability to read and write the components regarding the understanding of the environment of online information privacy which is represented in technology, regulations or common practices used to collect and share user's private information. The environment includes user's information on the computer that flows to all destinations such as Facebook, Twitter, etc (Correia and Compeau, 2017).

Some studies have discovered many users do not use and benefit the available advantage of the information privacy on social sites, for instance, more than 99% of Twitter users keep the default privacy settings where can user's name, list of followers, location, website, and biographical information able to be seen on their profiles. As well as Facebook users live with using default settings, the reason for that maybe users do not benefit from privacy options which are poor privacy settings interface, intricate privacy settings, and inherent trust, to overcome this problem, move toward to automatically father more appropriate default privacy settings have been suggested. PriMa automatically generates privacy policies, acknowledging the truth that the moderate user will find the assignment of individualizing his access control policies overpowering, due to the increasing complexity of online social networks and the variety of user content (Kayes and Lamnitchi, 2017).

Privacy attack is to know about the user's personal information by checking smart information grid network resources that information containing electricity consumption data bill where one can see the level of use of electricity over certain time periods might be used to conclude that the location is most probably not taken. Cybercriminals may decide physical attacks such as burglary and attack personal information on this information like credit card information that shared may be exposed to be targeted in a privacy attack. Millions of user accounts of a smart grid based on the internet of things also exposed to be at risk of a privacy attack. Nowadays, many techniques of hacking have been developed to attack the privacy information of internet users such as identity theft and information confidentiality. Therefore, it should protect the confidentiality and online privacy information of users from unauthorized access over the internet (Kimani et al., 2019). According to Basso et al. (2018) Privacy, policies are valueless if they are not implemented; which allows a variety of solutions to protect and save data of being attacked or unauthorized access. Applying the privacy preferences has defined before personal information of multitier applications exposé to be leaked at different levels such as starting from data storage to the user interface and policies may be executed at any scale. Nevertheless, when the privacy policies are enforced on data storage it will be protected better, but if policies are closer to the user it means to lead to giving a more chance to leak data.

Privacy behavior mentions to the variety of procedures that internet users apply to protect their information privacy on social networking. With time, users will become aware of the privacy risks that using online social media and the use of different techniques to protect and keep privacy (Heravi et al., 2018).

Parents are concerned about their children when using social networking, there are a variety of safe methods, reasonable and responsible tips for children to be in contact with the visible world of social networking. The first tip should be to set the correct privacy settings for the social account, parents should teach their kids to choose privacy settings that they have such as setting default sharing choice on their Facebook friends instead of public friends that they do not know, and always should motivate your children to do so. Secondly, think cautiously about what you are sharing on websites, that is very significant to be aware of any information you share over the internet, parents should teach their kids to be careful when they share or post any information that are sensitive, like photos and videos especially about their families and friends, which they would not wish to be seen by others on social media. Your children can use activity log to review things they tagged, this feature enabled by Facebook to help friends associated with each other. If something goes wrong, children can use the report violations of social networking of their terms, when they are confronted with something inconvenient on their social media accounts, they can make a decision to block or delete it. Get involved, there are a lot of great methods for children to keep in contact and react with people online on Facebook and Instagram about events and get involved in activities and invite friends. Build friendships, social media become a visual social club for people to meet and make friends, chatting with friends and have fun to play games online, to reduce stress after school and work, or social stress at home (Childnet international, 2016).

2.1.3 Perceptions of parents to use the internet

Parents should have tools that can assist them to monitor the time that their kids spend surfing on the internet. To monitor intelligently and carefully children's online activities in order to make parents realized clearly what their kids do on the internet. And allow efficient awareness of children's activity over the internet. Parents intend to direct their children to be responsible for the easy and safe use of the internet. But according to the study as presented that parents often do not keep an eye on their kids as they would wish to see. The feedback of the research showed that more than 50% of kids leave their social profile account for everyone on social media to view it. And more than 20% of the children do not realize the knowledge of making their account user privacy to private. Because of more than 12% of children have 100 friends in the contact list of their accounts, and have unprotected profiles. The research evaluated parents, the highest concern about the online activity of their children. Around 73% of parent's anxiety about their kids being communicated with strangers and viewing online unsuitable material such as pornography, this means there is a gap among parents that they are not conscious of kids' activities over the internet (Alqahtan et al., 2017).

According to Shin, (2015) parents shows that the internet has brought positive and negative impact on their kids. However, they see that the internet makes kids more positive effects of having knowledge of giving unlimited information and help children to get information easily and fast from the internet. The internet is a beneficial information source for the children to help them to do research on school duties that need internet information search. Parents are not too worried about their children to use the internet at this time. Some parents indicated that it is occasionally hard to prevent children from using the internet as it is addictive nature. But, they did not realize their kids were dangerous chronic to the internet as they organized the time that children spend on the internet at home, some parents have concerns about their children to see to child-unsuitable online material. Also, concerns about contact dangers on social media sites and privacy matters. Parents realize that a keyword typed on a search engine may lead children to undesirable outcomes on websites. Nevertheless, farthest worries were about thinking for the future, what will happen more than how kids surfing the internet nowadays. If parents do not care about monitoring the internet use of their children, they may be exposed to internet attacks.

2.1.4 The reliability of computer security software

The engineering of software reliability is an area where program development is related to putting the test and modeling the software capability to work efficiently and functionality of the environmental conditions over a specific period of time. There is no tool for development that can be warranted perfectly reliable software. There are techniques that are required for statistical modeling which allow the accomplished reliability to be estimated or predicted, which is based on monitoring of system insufficiency through system testing and operational process. There are seven distinct procedures that can be referenced in the software reliability engineering operation that consists of determining reliability objective, expectant system use, get ready test cases, performing the test, collecting fail data and severity levels, reliability growth modeling, dropping to field life, monitoring area performance (Driel et al., 2014).

As stated by the development constant of software reprocess technology besides the rising of the numeral and quality of open-source programs, also the likeness of the codes in various types of software is increased more and more. They reuse or larceny of program codes causes a problem of software identification reliability. Identity testimony contains the source code of the software, shared resource of software code, a guide to use, both configurations of software and hardware, an explanation of operation functionality environment, assistance document, etc. Through these impact elements, the software's source code is the most significant impersonation of the software identity. Also, some other proofs can be estimated through the review meeting technology. Meantime, many different studies present that a lot of multiplied code existing in huge code bases. Repetition may lead to bad programming exercise, because programmers oftentimes copy and paste code to quickly repeat functionality which may make superfine errors and create code that is hard to preserve (Yang et al., 2018).

The quality of software reliability is very important, with the use of spread software programs and applications, as a vital characteristic of computer software quality, because many programs contain a bug problem such as malware which leads to failures software, particularly for high-reliability software and embedded system programs. The reliability characteristic model is used as a frame to meet requirements of software reliability, which contain four characteristics, maturity, availability, fault tolerance, and recoverability maturity measures are applied to appreciate the stage to which the program meets the requirements of reliability under the natural process. Maturity measures represented the fault correction, MTBF (middle time among failures), failure average and test coverage. The fault correction characterizes what rate of detected reliability-related faults are validated. MTBF explains what the average time through failures within running the software process. Failure rate announces the rate size of failures existed within a given period of time. Test coverage characterizes the percentage of software capabilities or systems and functions which are absolutely executed in the test.

2.1.5 Self-efficacy for the safe use of the internet

The perception of self-efficacy is that if a person wishes to overcome potential problems, who should take the essential actions who believes in that. Furthermore, it is confirmed that the perception of self-efficacy appears to impact the right or wrong behavior of the person, besides how much stress he/she will set to resolve a problem as well as he wants to outdo the problem as Bandura (1977) determined the perception of self-efficacy for the first time in his paper. The perception of self-efficacy is a significant advantage in teaching and that more awareness should be made known. Individuals with a weak level of self-efficacy tend to make complicated things that make them panic and fall stressed (Cavus and Ercag, 2016).

With regards to realizing the students' self-efficacy and perceptions of the internet and computer utilization among genders independent samples t-test was used. Relating to the study of the self-efficacy and perception of the computer user and internet security, there are statistically considerable discrepancies between both males and females in this research ($p<.05$). The opinion of the outcome of the study shows that students have a perfect consciousness of computer and internet security as a general observation, however, particularly in idioms of malicious software, web security, and social networking sites, most of the students have a low level of awareness of them. The study would aid internet users to be able to access the safe use of the internet (Cavus and Mohammed, 2017).

According to Karabulut (2017), in his study, in these modern days, internet technology is popularly used everywhere around the world, so it is essential for users to be aware of safe use of the internet in order to prevent an unexpected online accident. Regarding the results of the research to characterize high school students' self-efficacy and perceptions of safe internet use in TRNC, the study shows that students have adequate awareness about the online security of social media. Nevertheless, the security of social engineering, computer security, and malware software are not perfect enough, they appear to be less than security measures that are required according to today's online security. The study specified a higher level of self-efficacy of internet users for those who surf the internet for more than 8 hours a day.

2.2 Theoretical Framework

2.2.1 Perceptions of parents towards the safe use of the internet

The safe surfing over online is very important for parents to be aware of online risks to protect their children in order to ensure the internet safety. Kids grow up in a technological age and parents should know unsuitable material that can affect online children's behavior such as violent pictures, pornographic images and online cheating of malicious users. Parents should have spare time to teach their children how to be safe online while surfing on the internet and never fill out their personal information online especially with those inappropriate websites. Children should understand to keep their sensitive information secret when they are online and do not try to send their personal information to anyone over the internet, for example, their names or upload pictures, mobile number, home address, bank account number, credit card, etc. In addition, children should not open any attachments of unknown emails which maybe include unsuitable pictures, pornography or even malicious software. Parents should tell their children to let them know about suspicious and annoyance users if they receive a message or a call from them, and can report or block inconvenience users on social media. More than 69% of parents and their children believe that the internet is not a safe place for kids. Should be addressed this perception to avoid online dangers, many chances are available that can be useful for children. But, when children surfing on the internet and they feel unsafe online, that means they do not admit the full online possibility. About 4.5% of parents think that the internet is a safe place, while children do not understand or realize that (Lauri, 2015).

Parents are perfectly unconscious of the risks that their children may be exposed to the danger of the internet, they think that they are able to control their children to use the internet only for no more than two hours. The internet dangers maybe consisting of serious content or harm behaviors that maybe come from online relationships among internet users. As reported by international discoveries of Marsh et al., (2015), parents should be aware of taking more attention to avoid and get rid of risky material (Bake and Tokes, 2018).

2.2.2 Privacy security

Privacy information is a very big issue and concern many people on social sites. Privacy arrangement settings of social networking can be debated in two ways, online privacy, and offline privacy. Online privacy means to dominate through data sharing with direct contacts of the user, for example, information that should be visional to whom, also known as access control management, or technique of users that can arrange their data and access control to it, also how it can be executed and ensured by the system. Offline privacy indicates to assure privacy-conscious control over the user's thoughts, behavior, tendency, emotions, and personality which can be taken out from a variety of analyzed collected data and meta-data which is created by utilizing social networking service over the internet. With the centralized model, online privacy is part of the services given by the online social networking provider. In online privacy, a user can see the direct inclusions and would be more worried about having his/her night party picture shown by some of his/her friends or workmates, instead of social networking provider siding him/her as a dejected person and maybe sell or share information with the third party. For that reason, online social networking providers have paid attention to develop their presented interfaces for privacy management over the internet. Users have noticed the improvement in the interface design of the privacy settings and functionality of social media like Facebook and Twitter. Online privacy management through the centralized model is more technical and easier, which can control all information, communication, and access channels from one place by the owner entirely to allow permission of access control to the data privacy (Bahri et al., 2018). Social networking has become an essential part of people's lives, where they can connect with family and friends by chatting, sharing photos, videos, and other information. But, people created content includes critical information of publisher that should not be seen by others, which leads to privacy violations of users' information shared. Many popular social media like Instagram and Pinterest are used to share photos, paralleled to literal information, images can transfer important information to the user, which is harmful to the people's privacy. Besides, the contents of the information may be exploit by a malicious attacker to acquire the victim's important information by photo processing.

Online social networking privacy policies are fundamentally about the users' data that will be scouted by the service provider, and which will allow a user to monitor the range of information sharing. Online social networking enables a privacy setting task for their users. The user has the right to choose and define which users have permission to access the shared image. The photo shared by the user may have linked to the others, which means a shared photo will be controlled by one user, and the privacy of other users who are associated with the photo may be exposed. Let us see this example, assume that Alice and Susan take a selfie photo of themselves, Alice shared the photo with other friends and her colleague Chris without Susan knowing. If Susan does not know Chris very well, then the image shared by Alice will be a privacy issue for Susan. In fact, the image owned by Alice and Susan, nobody has the right to share it without announcing it to his/her friend. Alice should have requested permission from Susan. For instance, Alice should avoid the privacy issue of the image shared by using editor pictures software in order to modify Susan's picture to be unclear for Chris to identify her face (Xu et al., 2019).

2.2.3 Information privacy concerns

The confidence of social networking users in companies based on their products and services. Facebook is a common trademark of social media used by more than 1.7 billion users around the world. The advertisements for information and data privacy violations by considerable organizations like Equifax and social networking massive, Facebook, may have raised users' privacy anxiety and declining customer trust in these companies. Facebook was exposed to harvest the personal information and opinions of users by Cambridge Analytica to offer alteration behavior services of users without permissions from owners. The unlicensed harvesting of users' profiles on Facebook to raise privacy worries of users and to make trustiness problems for Facebook. Facebook's Manager was asked by the United States Congress about users' concerns and to assure them to keep their information safe, also motivate them not to lock their facebook accounts. In 2018 Facebook decided to buy fully advertisement pages from different organizations in order to present an apology to their customers. In spite of that, as a research study of Ayaburi and Treku (2020) large markets in Germany and the United States of America referenced that users preserved a minimum level of confidence in social networking, particularly on

Facebook users' privacy, as well as some users rethink their memberships on some social networking sites. Through platforms of social networking, regarding repeated information and privacy contraventions related to digital data, it is noticeable that influences on the procedures of social networking trademarks or institutions are very complicated and regulation parallel to communication convention. We suppose two hypotheses of possibility interposition tracks in the theoretical sample. First, To be an internet fraud victim is anticipated to interpose the consequences of the first phase measures of self-discipline and internet activities regularly on internet privacy anxieties. Online privacy worries are anticipated to mediate the impact of being an internet fraud victim on the fourth-step privacy defense behavior changeable (setup and updating antivirus software, password changing repetition) (Chen et al., 2017). Predictably, dangerous privacy and security issues appeared, which is defined in two major types of attacks. Attacks that use the implied confidence embedded in announced social relationships, and attacks that harvest the personal information of the user for evil-destined usage (Kayes and Lamnitchi, 2017). Social media such as Facebook is the farthest communal used among internet users, together with the increasing of social networking improvement and commonly the problem of information privacy worries have gained people's attention and awareness of internet users (Kusyanti et al., 2017). On social media Twitter, users are worried about their tweets more than others sharing their own information with other users through retweets. It could be constructional of social media between Facebook and Twitter, where Facebook, a society is created around one network and social interaction, while the idea of Twitter concentrates on transmitting information to the overall public, which allows other users to see the tweet of any user on Twitter (Jeong and Kim, 2017). The new technologies of information represented in artificial intelligence, the fifth generation of communications, data analytics and the internet of things have simplified many chances and changes in the business and social circumference, which became an exporter of intelligence and new commerce paradigm for individuals, businessmen, institutions, and politics agencies that let gathering and analysis of data over the internet from the websites, social networking, and e-business platforms. Nevertheless, probably data were assembled for large data analysis is potential to be critical personal information for individuals' behavior, habits, and activities of their daily lives, sensitive information can be privacy concern issues of people’s information, it maybe makes conflict with introducing the best services to the community (Lee et al., 2019).

2.2.4 Internet security threats

1. Computer security threats

Computer security threats are a potential threats that exploit vulnerabilities in a computer or network, such as bugs injected to harm the computer systems.

- **Malicious software**

Malicious software is a programming code embedded in the software that is made to damage a computer system or to attacks computer networks in order to affect computer security, malware comes in a variety of forms such as computer viruses, worms, trojans, adware, and spyware (Ozdamli and Ercag, 2019).

- **Computer viruses**

The computer virus is an execution code of a malware program embedded in trusted computer software, that can make copies of oneself to be extended in executable files, in order to damage and delete the computer programs, files, and documents. Viruses transfer from an infected computer system to another uninfected computer system, especially through computer networks when sharing programs and files among computer users (Tasril et al., 2017).

- **Trojan horses**

A Trojan horse is a malicious program that pretends to be as a legitimate and trusted software to trick the victims to install it on their computer systems, the trojan is invisibly included in an application and it starts executing when the software is running. The cyber hackers use it to access information of the computer and harm the target systems of the victims (Namanya et al., 2018).

- **Worms**

Worms are malicious software that works on duplicating themselves to spread into a computer network through vulnerabilities in the targeted systems, for the purpose of affecting the security of the computer and causing harm to the network system that may lead to a denial of service (Mirza et al., 2014).

- **Spyware**

Spyware is a type of malware program that is created by internet hackers to access the computer system to gain sensitive information of the victim without being known in order to collected and transferred data to the cybercriminal, which may be used for illegal targets, such as personal identifying information, passport information, student information, bank account, passwords, credit and debit cards, and medical insurance information (Tasril et al., 2017).

- **Adware**

Adware is a software that appears on the user interface to present undesirable advertisements that maybe contain harmful software used to steal a user's important information. Adware is represented in web pages in the form of a pop-up ad or other forms, which include advertising of a product's promotion contains commercial, educational and shopping advertisements, etc, which attract the attention of the user (Namanya et al., 2018).

- **Ransomware**

Ransomware is a type of malware that is requesting a ransom payment from the victims after taking control of their documents, files, personal information and preventing them to access their computer systems unless they pay ransom to the attacker. Ransomware makes threats to publish important information of the user or to make the denial of service of the system forever. In addition, the ransomware attack blackmails the victims to send their data to illegal users or other internet criminals that may be used in the wrong way, unless the request is paid to the attackers (Buch et al., 2018).

- **Rootkits**

A rootkit is a variety of malware programs of a computer that is developed to be able to access the computer systems to cause harm and damage to the file system and disable computer software such as an anti-virus. The rootkit is hidden and running in the background without the user's knowledge (Zeidanloo et al., 2016).

2. Online cybercrime

Cybercrime is a criminal act of unauthorized access to the computer system, computer network, and other internet devices, for the purpose of gaining access to sensitive information of victims of cybercrime, which can be targeted to individuals and organizations. Cybercrime is done by hackers and cybercriminals by using the hack tools or writing a code programming to take control of the computer system that can be easy to spread malicious software through it, to commit many types of cybercrime include damage files and documents or to encrypt them, denial of service attacks, ransomware, spread illegal information and hate speech, racism, and exploit child pornography.

According to Nouh et al. (2019) as the European Commission suggested that cybercrime is criminal hacking actions that have been committed to attacking information systems and communications networks systems.

- **Phishing**

Phishing is a method used to steal personal crucial information from the victim’s computer through disguising as a legal way to gain data that contains bank account, credit card, username, and password (Buch et al., 2018).

According to Parsons et al. (2019) in his article, he defined phishing as a form of cheating to steal personal data and critical information over social engineering techniques by using an email. Hackers can send emails and behave as a trustworthy user by driving victims to click on a link or to open an attachment email which includes malicious software to send information of victims to the attackers.

- **Identity theft**

Identity theft is another type of cybercrime that aims at obtaining the identification information of a person or people to be used by the attacker to steal essential data of another person who is a victim in order to make illegal processes such as getting financial data, transfer money, online purchases or other online crimes. Identity theft intends to gain the personal data of the user represented in name, identifying the national number, username, password, bank account, credit card without his or her knowledge or without his or her consent to use the information, to commit cybercrime (Yuan et al., 2018).

- **Hacking**

Hacking is an attack on the computer system and networks through unauthorized access to the computer information systems for the purpose of controlling the computer security system to spread malicious programs to get sensitive information of victims and retrieve it to the hackers, or to damage files and documents, usually, the hacker uses bugs of security systems to hack a computer (Buch et al., 2018).

- **Spreading hate and inciting terrorism**

Spreading hate and inciting terrorism is extremely popular used as mechanism aggressive activities of an ideology of hate speech to achieve the goals of a group or organization. In the past, it was used to spread hate speech by traditional social media, for example, TV, Radio, Magazine, Newspapers. In these modern days, they use online social media like Facebook, Twitter, and YouTube to harass people because speech is the communication language to communicate opinions, ideas, concepts, attitudes, and beliefs (Chetty and Alathur, 2018).

- **Child pornography**

Child pornography is a pornographic material used to take advantage of children for sexual excitation that can be created with a direct partnership or sexual violation of children. Also, simulated Child pornography is classified as sexual abuse (Ngejane, 2018).

- **Grooming**

Child grooming or known as (sexual grooming) is a connection operation that is done by an offender that applies relationship searching strategies. Concurrently attracting in sexual sensation and information gaining of victims for the purpose of improving relationships which leads to the achievement of the needs of the result such as physical sexual temptation (Ngejane, 2018).

- **Denial-of-service attacks**

Denial-of-service attacks have used the internet to target sites over the internet. The DDoS attack is designed to prevent legal users to access their resources of the network via sending undesirable traffic to the computers and networks of the victims to exhaust services widely connection. The rising use of the Denial-of-service attacks is made the online servers at a huge risk (Somani et al., 2017).

2.2.5 Online safety tips for parents to educate their children on internet safety

These are many important online safety tips for parents to abide by in order to safeguard internet surfing.

- **Parents should use protection tools or parental control programs for monitoring children's online activities**

The use of parental control software or online protection tools assists parents to know how to control inappropriate materials or contents, such as websites and counterfeit advertisements which include malicious programs. Parental control programs help parents to have a familiarity with the online activities of their kids, for example, control internet usage time, or visited websites, block sites, restrict send or receive emails, tracking malicious websites or links, and report unsuitable online activities. These programs work highly efficiently to keep safeguard children's online behavior. Parents should teach their kids to cover the webcam of their computers when it is not in use because it can be used by hackers to take photos of your computer's screen, which may be used for threat (Benson, 2019).

- **Parents should educate children about online privacy information**

Parents must be aware of the importance of educating their kids about the world of the internet. For instance, what are the advantages and disadvantages of the internet, benefits of learning on the internet, social media sites, Facebook, Twitter, how to be safe on the internet, what is cyber security, give an explanation of different forms of online cybercrime, the importance of online privacy. Parents should be aware of teaching their children the risks of social media, and to set privacy security at a higher level for security purposes. Kids should be told not to send personal information to any websites especially the unknown sites, or to post photos or videos of their family and friends that may give an inappropriate expression on social networking. Also, educate them not to fill out personal information details of their profiles on social media accounts or to share them with others, parents should tell kids to be conscious of never to trust anyone of their friends to promise to meet online or in real life without parent awareness, they should not reply to any threats from emails, messages, or answer to unknown video calls, and to post feedback or tweet without consent and knowledge of their parents. Also, parents should teach children to be careful of online fraud from hackers, not to reply to them and not to send them their personal information like name, phone number, home address, password, credit card number, etc. Parents should teach their children to let them know when they surf online and see inconvenient materials such as pictures or videos, and when they feel unsafe on the website, they should turn off the computer and ask their parents for help immediately (Shin and Kang, 2016; Benson, 2019).

- **Parents should help children to make strong passwords**

Parents should teach kids how to create a strong password, make the password as much as possible to be complex and to create long passwords to be hard to hack by hackers, and it should be changed regularly, set a password in different combinations using letters, symbols, and numbers. Also, do not use the same password with different emails and accounts especially on social media, and never give the password to everyone except parents to be saved for any emergency situation. Children should learn not to use their mother's or father's name, and their phone numbers as a password, for it may be easy to hack (Benson, 2019).

- **Parents should listen and learn from their children**

The best way to get information about the online activities of children is to let children teach you what they have learned from the internet, how they are surfing on the websites, how they use text, post, and chat messages with friends on social media, how they open youtube videos. Parents should be patient and pretend in front of their kids that they do not know too much knowledge of the internet, and they wish to learn from their kids everything that they have learned and discovered from the internet parents need to be aware of educating their children about modern technology for the purpose of protecting children from the negative effects of attracting dangerous online activity and learn how to be safe against cyberbullying (Almagor, 2018).

- **Parents should limit the time that their children spend on the internet**

Parents should focus on the time that their kids spend on the internet, and what they should do and should not do on the internet, let them know obviously that they should spend limited time only to surf online or to search for solving problems on their homework after school. Make sure that they do not allow them to spend hours the internet (Kang, 2018).

- **Parents should help kids to install antivirus software, anti-malware, anti-spyware and to update them regularly**

It is very important to install an antivirus program and it should be licensed from a trusted company to ensure it works effectively and does not contain malicious software. Teach your kids to scan their computers against viruses, worms, and the likes. And also, tell them to scan for viruses or malicious software before downloading programs, files, videos from unknown/untrusted websites, and to update the antivirus regularly (Schleicher, 2019).

- **Parents should secure a home Wi-Fi network, and tell kids to disconnect with unsecured wireless networks in public places.**

Tell kids to reset the Wi-Fi password and make it a strong password to prevent hackers to hack their Wi-Fi in order to steal sensitive information, tell them to be careful when they are outside home at shopping centers , cafe, or at restaurants and not to connect with public Wi-Fi networks which may be unprotected from unauthorized access by hackers (Schleicher, 2019).

- **Parents should educate children about online habits and hate speech on social media.**

Parents should be aware of teaching their children to avoid participating in spreading hate speech or racism words which they see in videos and images in some pages on social media sites or to write harsh comments against other people's opinions on some issues, and also learn to differentiate between fake news and real news (Chetty and Alathur, 2019).

- **Parents should educate kids about online violence.**

The virtual world is growing day by day, especially playing violence games that have an effect on children. Parents should make children conscious of online game risks that may contain games depicting violence, which may have consequences on children's behavior, such as violent acts, nightmares from the games may make children paranoid. Parents should not play such games in front of their children (Kang, 2018).

- **Being digital citizenship.**

Parents should be aware of educating kids to be safe online and connect with an online safe environment to be digital citizenship. The common digital citizenship educates students 'diversity of technology topics, such as online safety, privacy and security, cyberbullying, information literacy, and digital drama. The standard scenery suggests that digital citizenship is "the criterion of suitable, responsible technology utility" (Gleason and Gillern, 2018).

- Make some time to spend online together with your children to educating children on suitable online behavior and help them to Bookmark their favorites websites in order to get easy access to the sites.
- Parents should be keen on seeing and monitoring their children's computers or devices such as smartphones and tablets so as to notice easily what their kids are doing online and not to let them use it in their bedrooms for a long time.
- Children sometimes forget to log out of their social media account especially when they use their friends' mobile phones or computer, or someone else devices. Parent should remind them not to leave their accounts without logging out when they do not want to use it.
- Ask your children to delete or block an invitation request of an undesirable friend or unknown person when they receive it on social media such a Facebook.
- All social networking have terms and conditions to use for online safety. Parents should always tell and encourage their children to read carefully and to be careful the terms and conditions of online applications and sites.

CHAPTER 3

RESEARCH METHODOLOGY

This chapter explains the particular methods used for the study. It encompasses research model, participants, data collection procedure, data analysis as well as the reliability test of the instruments used.

3.1 Research Model of the Study

The essential purpose of this research is to investigate the awareness of parents towards the online safety use. Particularly, it determines the awareness between parents towards the safe surfing over online in the Turkish Republic of Cyprus. The independent variable of the research and descriptive study contains five variables: relative relationship, age, education level, internet connection, and devices use online. The dependent variables consist of different items in the questionnaire such as online security measures, protection of information privacy, internet security vulnerabilities, reliability of computer security software. The research questionnaire comprises 53 items as explained in Figure 3.1.

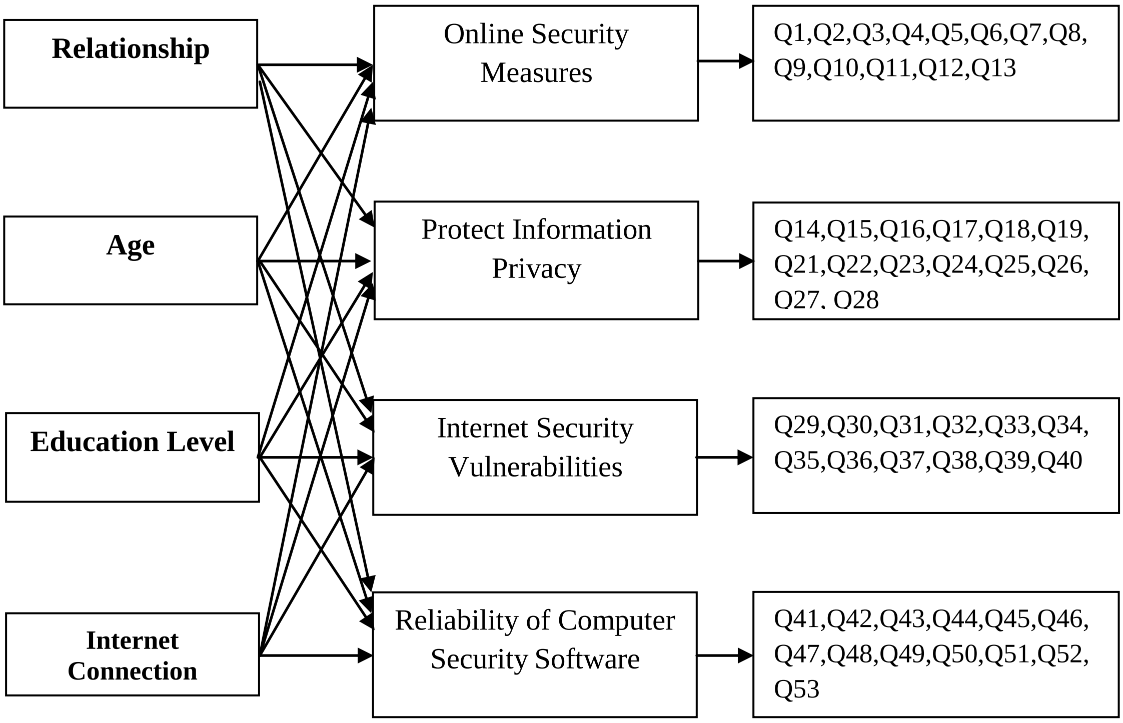

Relationship
Age
Education Level
Internet Connection
Online Security Measures
Protect Information Privacy
Internet Security Vulnerabilities
Reliability of Computer Security Software
Q1,Q2,Q3,Q4,Q5,Q6,Q7,Q8, Q9,Q10,Q11,Q12,Q13
Q14,Q15,Q16,Q17,Q18,Q19, Q21,Q22,Q23,Q24,Q25,Q26, Q27, Q28
Q29,Q30,Q31,Q32,Q33,Q34, Q35,Q36,Q37,Q38,Q39,Q40
Q41,Q42,Q43,Q44,Q45,Q46, Q47,Q48,Q49,Q50,Q51,Q52, Q53

Figure 3.1: Research model of the study

3.2 Research Participants

The volunteer participants in this research were parents of the children at the Near East Libyan school. The research was conducted during the 2018-2019 summer and 2019-2020 fall terms. The samples of the questionnaire have been distributed to the children at the schools in order to be given to the participants (their parents). This study consists of a total of 252 samples for parents, and the respondents were chosen randomly from different related of relationship, age, education level, internet connection methods, and devices use to get online, which are made up of 116 fathers and 136 mothers. The education level of Bachelor/High Diploma was 38.9% of the parents, and the education level of Master and PhD degrees were 61.1% of the parents. The majority use of the internet connection methods were used to connect to the internet was 55.1% of parents use Wi-Fi, and 36.8% of parents used 3G to get online, and 5.6% of respondents used ADSL connection, and

2.5% of parents used Cables. The important characteristics of the participants are presented in Table 3.1.

Table 3.1: Demographic information of survey participants (N = 280)

Characteristic Relationship	**Frequency**	**Percentages**
Father	116	46.0
Mother	136	54.0
Age		
20 – 39	177	70.2
40 – 69	75	29.8
Education Level		
Bachelor/High Diploma	98	38.9
Master/PhD	154	61.1
Internet connection use		
Cable	10	2.5
ADSL	22	5.6
3G	145	36.8
Wi-Fi	217	55.1
Devices use to get online		
Desktop Computers	35	7.4
Laptop Computers	154	32.5
Mobile Phones	219	46.2
Tablets	66	13.9

3.3 Data Collection Tools

The questionnaire sample was used to collect data of the research from the respondents, the questionnaire was developed by the researcher in order to determine the awareness of parents towards secure surfing through the internet. It is comprised of three sections as shown in Figure 3.2 bellow.

Section1 Demographic Information of the Participants: This section contains the data information of respondents such as Relative relation (parents), Age, Education level, How to access the internet connection and Which devices use to get online as explained in Figure 3.2.

Section2 The knowledge Questions of the Participants: This section assessed the knowledge of the parents about their children's online activities.

Section3 Awareness of Internet Security: This section explored the awareness of parents towards online safety. It consisted of four parts containing a total of 53 items that comprised of essential measures of online security, protect information privacy on websites, internet security vulnerabilities, and reliability of computer security software. The respondents provided answers to the items based on 5 Likert-type scales from Strongly Agree (5 points), Agree (4 points), Neutral (3 points), Disagree (2 points) and Strongly Disagree (1 point).

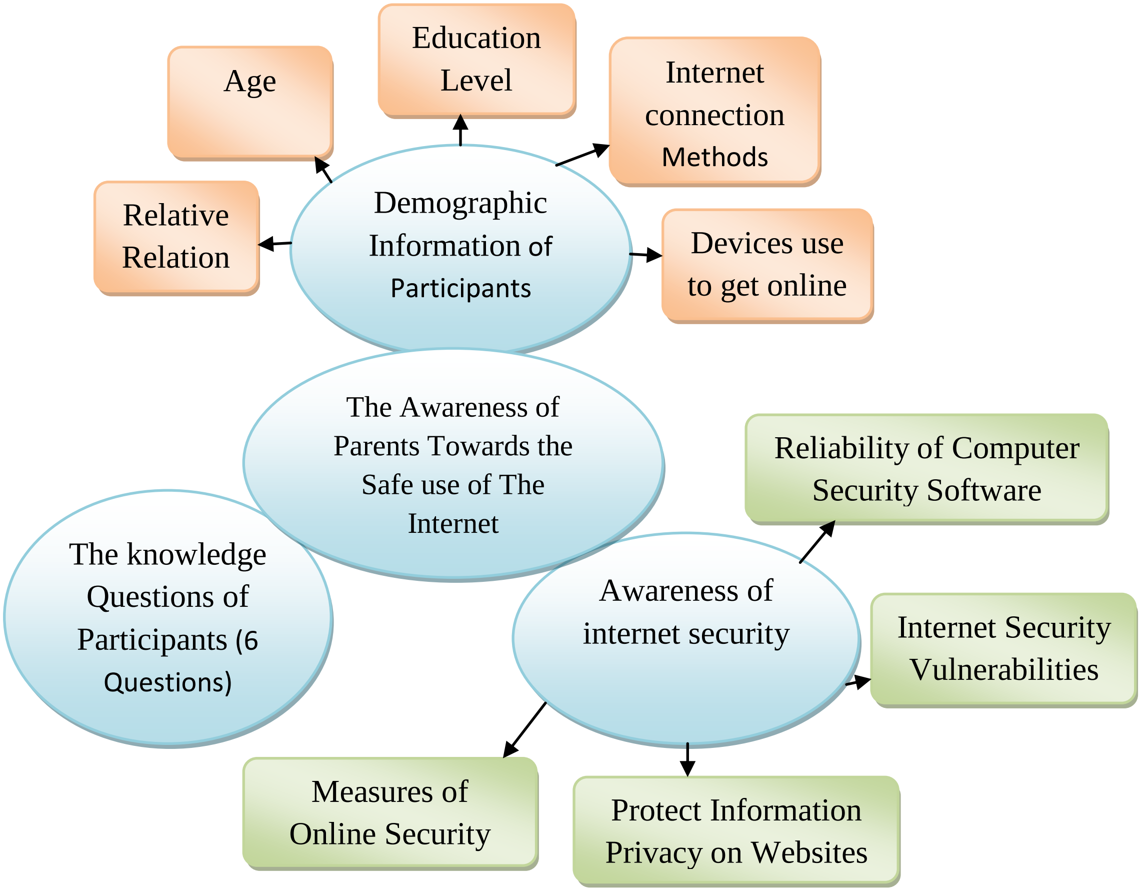

Age
Education Level
Internet connection Methods
Relative Relation
Demographic Information of Participants
Devices use to get online
The Awareness of Parents Towards the Safe use of The Internet
Reliability of Computer Security Software
The knowledge Questions of Participants (6 Questions)
Awareness of internet security
Internet Security Vulnerabilities
Measures of Online Security
Protect Information Privacy on Websites

Figure 3.2: The structure of the questionnaire

3.4 Reliability Test of Survey Dimensions

The data questionnaire was analyzed to confirm the reliability of the questionnaire scales which was calculated by using Cronbach’s Alpha for all 53 items of the questionnaire. Also, the total results of each scale and coefficient of the reliability test were more than 0.700 and the overall results of dimensions were 0.843. According to the reliability test for subscales. The highest dimension of Alpha test result was .718 on the scale of essential measures of online security and the lowest result was .709 for dimension of protect information privacy on websites which can be noticed the Cronbach’s Alpha test results between dimensions that were interpreted below in Table 3.2 of the scales.

Table 3.2: Cronbach’s Alpha for the questionnaire dimensions

Dimensions	**N of Items**	**Cronbach’s Alpha**
Essential Measures of Online Security	13	.718
Protect Information Privacy on Websites	15	.709
Internet Security Vulnerabilities	12	.713
The Reliability of Computer Security Software	13	.714
Cronbach’s Alpha for Overall Items	**53**	**.843**

3.5 Research Procedure of the Study

The purpose of this study is to investigate the awareness of parents towards online security use . The questionnaire sample used comprised of three sections, demographic information, knowledge questions, and awareness of internet security software, and it contained a total of 53 items. divided into four factors. Samples were prepared and printed out to be distributed to the voluntary participants (Parents) through their children at Near East Libyan school. A total of 280 copies of questionnaire samples were distributed to the participants for one month and data were collected. The number of the responded questionnaire was 252 and verified to be valid. The returning questionnaires sample of hard copies were examined and checked to eliminate errors of data to ensure the quality of data and was analyzed by SPSS software version 25.0. The data were subjected to diverse analyses frequency, percentage and independent t-test. In other words, the results acquired in the study were described and interpreted in the tables and figures were explained in the research. The time spent each task to achieve the study is tabulated in Table 3.3 below.

Table 3.3: Time schedule of the research

Procedure	**Duration Time**
Finding the topic and writing a proposal	2 Weeks
Literature review	2 Weeks
Preparing and designing the questionnaire sample	2 Weeks
Ethics approval for the questionnaire sample	6 Weeks
Distributing the samples to the participants	6 Weeks
Data Collection	9 Weeks
Entering and data Analysis in SPSS software	5 Weeks
Complete the chapters (During the research one by one)	5 Weeks
Submission the thesis to the supervisor	2 Weeks
Total	**39 Weeks**

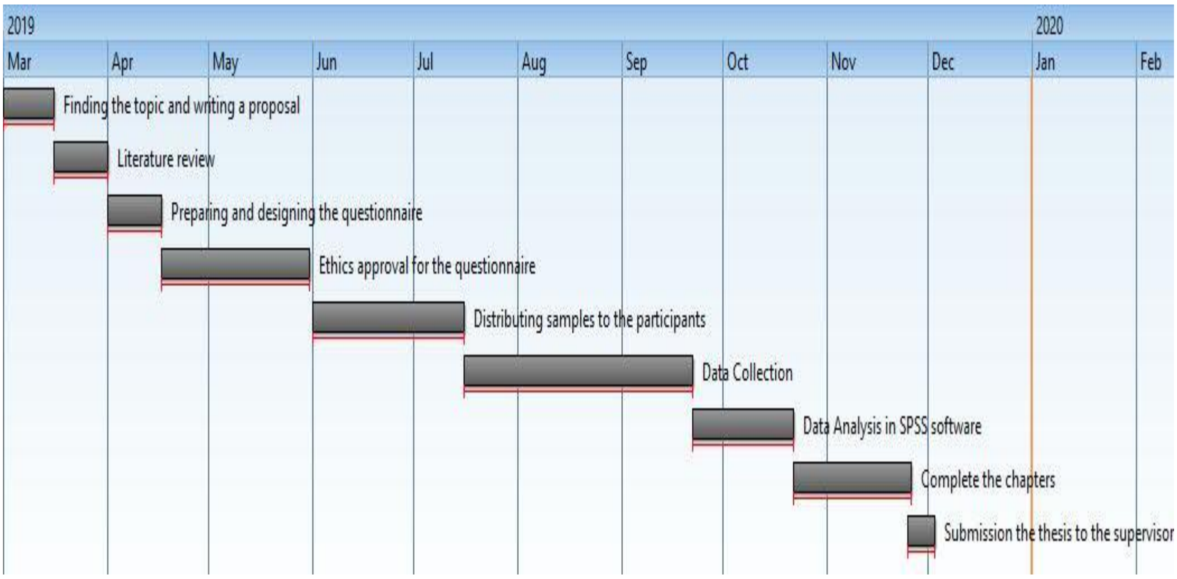


Figure 3.3: Gantt chart of the research

CHAPTER 4

RESULTS AND DISCUSSION

This chapter is to discuss the results of the research and to give a description and interpretation of the consequence of this study such as descriptive statistics and dependencies etc. For the purpose of understanding the awareness of parents towards the safe surfing over the internet, as the results described and shown in tables.

4.1 The Knowledge of Parents About Their Children's Internet Use

According to the results in Table 4.1 more than half of the parents claimed they know their children online passwords (54.4%), the hours their children spend chatting online per week (53.6%). More than one-third (36.1%,) of the parents use internet filtering software on all computer accessible to their children. 138 of the respondents representing 54.8% have online rules agreements with their kids. More than two-fifth (44.8%,) claimed their children have knowledge of safety tips.

Table 4.1: The knowledge of parents about their children's internet use

Questions	**Yes**		**No**	
	N	**%**	**N**	**%**
Do you know your children's online passwords	138	54.8	114	45.2
Do you know how many hours a week your child spends chatting online with others	135	53.6	117	46.4
Do you use internet filtering software on all computers your child has access to	91	36.1	161	63.9
Do you have an online rules agreement with your child	138	54.8	114	45.2
Is the computer your child uses kept in a high traffic area in your home	103	40.9	149	59.1
Does your child know of the safety tips	113	44.8	139	55.2

4.2 Parents' Use of Internet Connection Access Types

Regarding the statistical analysis, the results presented in Table 4.2 shows the internet connection method used to access to the internet among participants for purpose of understanding the awareness of parents towards online security utilize.

Table 4.2: Parents' internet connection access types

Internet Connection Use	Use		Not use	
	N	%	N	%
Cable	10	4.0	242	96.0
ADSL	22	8.7	230	91.3
3G	145	57.5	107	42.5
WI-FI	217	86.1	35	13.9

Descriptive statistics were performed to check the differences of parents' internet connection use. Wi-Fi internet connection has the highest percentage, constituting 86.1% of parents, whereas Cable has the lowest percentage representing 4.0% of parents.

4.3 Devices Used of Parents to Get Online

The results obtained in Table 4.3 describe the devices that parents use for online connection in order to examine the awareness of parents towards the safe surfing over the internet. The descriptive statistics was applied to see the differences between devices which parents used to get online.

Table 4.3: The devices used by parents to get online

Devices use to get online	Use		Not use	
	N	%	N	%
Desktop Computers	35	13.9	217	86.1
Laptop Computers	154	61.1	98	38.9
Phones Mobile	219	86.9	33	13.1
Tables	66	26.2	186	73.8

The results revealed that the majority of parents (86.9%) make use of the mobile phones device whereas only 35 parents representing 13.9% use desktop computers to get online.

4.4 The Awareness of Parents Towards the Safe Use of the Internet

The statistical analysis was executed on all items of the dimensions in order to examine the awareness parents towards the safeguard through the internet where the highest mean obtained from the participants' response 3.21. The results of differences from the statistical analysis of the mean and standard deviation of each item was presented in Table 4.4.

Table 4.4: Explains the awareness of parents towards the safe use of the internet

Items	Mean	SD
Essential Measures of Online Security		
1. I am conscious of the importance of online internet security software.	2.69	1.07
2. I am aware of the riskiness malicious software attacks.	2.65	1.32
3. I am conscious of purchasing internet security software from trusted online websites.	2.64	1.28
4. I do not concern to share my account password with my friends and family on social media.	3.08	1.52
5. I am aware that some of the Internet Security Software contains malware programs.	2.62	1.22
6. I am not careful to install any internet security software of any resources on the internet.	3.11	1.23
7. I am aware of the cybercrime attacks that threats people's data on the internet.	3.12	1.17
8. I have not been learned of keeping personal information secret over the internet.	3.15	1.26
9. I am aware to be able to share legal information with trust people on the internet.	2.67	1.12
10. I use a unique username and password for all my accounts on social networking.	3.03	1.40
11. I am aware of Microsoft recommendations for creating a strong password.	2.64	1.17
12. I do not respond to any mysterious requests from a stranger friend on social media.	2.22	1.13
13. I know it is difficult, to be honest with anyone on online chatting.	2.15	1.14
Protect Information Privacy on Websites		
14. I am aware of applying information privacy policies on social networking against phishing sites.	3.10	1.29
15. I know I should not fill out sensitive data of my profile account on social networking.	3.11	1.35
16. I Make a complex, unique password and change it every 90 days.	3.13	1.15
17. I am careful about what I share on social media with others.	3.24	1.30
18. I am careful to avoid posting controversial information on social media.	3.29	1.20
19. I am aware that unknown emails addresses may include malware	3.07	1.36

links.		
20. I am not conscious of phishing emails used to convince the victims to send sensitive information.	3.28	1.12
21. I do not care about leaving my confidential information exposed to be shared on social sites.	4.01	1.02
22. I used to enable and strict privacy settings on social media and websites.	3.02	1.18
23. I run the firewall on and update antivirus software while I am surfing online.	3.11	1.19
24. I have never click on malicious links that are able to infect my social account.	3.02	1.26
25. I am aware of the responsibility for online communication and activities through posting and sharing on chat rooms and emails.	3.00	1.24
26. I make online shopping and purchase from secure sites.	3.07	1.30
27. I am not able to teach my children how to use the filtering, privacy and safety settings on websites.	3.35	1.16
28. I will not share and comment on any person or website spread pornographic materials on social sites.	3.24	1.32
Internet Security Vulnerabilities		
29. I have replied to a link that I received on an email and I sent my user account credentials.	3.12	1.41
30. My computer system has stopped working by a denial-of-service attack	3.15	1.22
31. I use a username and strong password to login on my computer system	2.38	1.16
32. Using security software tools and services for transferring large data over the internet.	2.62	1.24
33. I use internet security programs against architectural weakness of the computer system.	2.64	1.08
34. I am unaware of using the firewall to control inbound and outbound of internet traffic.	2.68	1.10
35. I lost sensitive data without my early knowledge.	3.50	1.16
36. My files have been encrypted by malicious ransomware programs.	3.56	1.22
37. Implementing anti-spyware software against Internet threats.	2.81	1.18
38. I have clicked on a download link and I realized it installed a malware.	3.04	1.18
39. I use anti-malware software, ad-blockers and apply safety settings filters to deny access to undesirable content on websites.	2.36	0.98
40. I am concerned when I click by mistake on a questionable advertisement on a website page.	2.18	1.04
Reliability of Computer Security Software		
41. Use the latest version of the Anti-virus software and ensure it up to date	3.01	1.34
42. Implementing anti-spyware software against internet security threats on the computer system.	2.62	1.18
43. Computer system shows a message attack of a malware software "Your machine is not affected".	2.61	1.22

44. I make Regularly backup data to be protected from viruses, worms, ransomware, spyware, and Trojan.	2.32	1.14
45. I make a backup of sensitive information to be saved in a safe place	2.65	1.26
46. I am not aware of using the reliability and quality of security software on computer.	3.05	1.30
47. My files and documents were damaged because of some programs contain Computer viruses and worms.	3.01	1.30
48. My computer programs are illegal as it downloaded from untrusted websites.	3.05	1.29
49. My computer files were exposed to ransomware software attacks.	2.75	1.25
50. I make back up data for an emergency case of malware attacks.	2.06	.96
51. I am aware to use highly efficient and reliability of internet security software.	2.20	.94
52. I am unaware that some of the security software I installed on my computer contains malware and spyware.	3.04	1.19
53. I use software to prevent my child to access unsuitable websites.	3.09	1.28

According to the results above in Table 4.4 explains the highest mean of the respondents on the items of the questionnaire that was enrolled in item 21 “I do not care about leaving my confidential information exposed to be shared on social sites” (M=4.01, SD=1.02). This is result is an indicator that parents have good knowledge and awareness of keeping their private information confidentially on social networking sites. The second highest mean on the items was recorded for item 36 “My files have been encrypted by malicious ransomware programs” (M=3.56, SD= 1.22). And the third highest mean of the items was recorded for item 35 “I lost sensitive data without my early knowledge” (M=3.50, SD= 1.16). The lowest mean response on the questionnaire items was recorded on item 50 “I make back up data for an emergency case of malware attacks” (M=2.06, SD=.96). That response could be reflecting the low awareness among parents about making backup data for important information and maybe they are not aware of malware attacks and other types of viruses. The second lowest mean on the items was recorded for item 40 “I am concerned when I click by mistake on a questionable advertisement on a website page” (M=2.18, SD=1.04). And the third lowest mean of the items was recorded for item 13 “I know it is difficult, to be honest with anyone on online chatting” (M=2.15, SD=1.14), the Table 4.5 shows the total Mean and Std. Deviation of each dimension of the questionnaire.

Table 4.5: The total mean scores of each factor

Dimension	Mean	SD
Essential Measures of Online Security	2.75	.59389
Protect Information Privacy on Websites	3.20	.54975
Internet Security Vulnerabilities	2.84	.57577
The Reliability of Computer Security Software	2.73	.57675

4.5 The Difference Between Parents' Awareness Towards the Safe Use of the Internet Based on Relative Relationship Difference

According to statistical analysis, results illustrate an indication of the parents' awareness towards the safe use of the internet based on relative relationship variable differences and all dimension of the questionnaire, the independent-samples t-test was conducted to analyze the result which is interpreted in Table 4.6 provides an overview of parents' awareness and perceptions towards the safe use of the internet.

Table 4.6: The difference between parents' awareness towards the safe use of the internet based on relative relationship difference

Dimensions	relationship Variable	N	Mean	SD	Mean difference	t	P
Measures of Online Security	Father Mother	116 136	2.70 2.80	.62759 .56137	-.10516	-1.404	.162
Protect Information Privacy	Father Mother	116 136	3.23 3.18	.53192 .56563	.04509	.652	.515
Internet Security Vulnerabilities	Father Mother	116 136	2.86 2.81	.58376 .57020	.04509	.619	.537
Reliability of Computer Software	Father Mother	116 136	2.72 2.74	.60434 .55420	-.02077	.284	.776

The statistical analysis shows that Fathers parental were recorded the highest Mean value of (M = 3.23; SD = .53192), and Mothers parental were shown the lowest value of (M = 3.18; SD =.56563), The results confirmed that there are no statistically significant differences between parents on all dimensions (p>0.05). The results in this study were compared with the study of (Cavus and Mohammed, 2017) reported that there were a statistically significant differences between genders in the study, it shows that there is a different statistically significant with this study in related to online safe use.

4.6 The Difference Between Parents' Awareness Towards the Safe Use of the Internet Based on Age Groups Difference

According to results from the statistical analysis showed the differences between parents' awareness towards the safe use of the internet based on Age groups variable difference with all dimension. The independent-sample t-test was used to analyze the result as was explained in Table 4.7.

Table 4.7: The difference between parents' awareness towards the safe use of the internet based on age groups difference

Dimensions	Age groups Variables	N	Mean	SD	Mean difference	t	p
Measures of Online Security	20-39 40-69	177 75	2.84 2.54	.54005 .66103	-.10516	3.812	.000
Protect Information Privacy	20-39 40-69	177 75	3.22 3.15	.53171 .59041	.04533	1.003	.317
Internet Security Vulnerabilities	20-39 40-69	177 75	2.85 2.81	.53231 .67060	.04509	.429	.668
Reliability of Computer Software	20-39 40-69	177 75	2.77 2.63	.55670 .61416	-.02077	1.771	.078

The age group of 20-39 have the highest Mean value of (M = 3.22; SD = .53171), and the Age group of 40-69 have the lowest value of (M = 3.15; SD =.59041) according to that the Age groups of parents have founded that there is no statistically significant differences on protect information privacy on websites and internet security vulnerabilities dimension with both Age groups of parents ($p>0.05$). However, there is a statistically significant differences on essential measures of online security and reliability of computer security software dimensions ($p<0.05$). The research shows that there is a similar results was researched in the study was conducted by (Cavus and Mohammed, 2017) was reported that there is a statistically significant differences in all ages. Also, according to Patrick et al., (2018) has found that there was statistically significant in age variable related to online activities.

4.7 The Difference Between Parents' Awareness Towards Online Safety Use Based on Education level Difference

Results in Table 4.8 illustrates that parents' awareness towards online security use based on age groups variable differences on all dimension. The independent-samples t-test was employed to analyze the result that was shown in Table 4.8.

Table 4.8: The difference between parents' awareness towards the internet security use based on education level difference

Dimensions	Education level Variables	N	Mean	SD	Mean difference	t	p
Measures of Online Security	Bachelor/High Diploma Master/PhD	98 154	2.79 2.73	.59266 .59558	.05594	.728	.467
Protect Information Privacy	Bachelor/High Diploma Master/PhD	98 154	3.21 3.20	.53909 .55815	.00835	.117	.907
Internet Security Vulnerabilities	Bachelor/High Diploma Master/PhD	98 154	2.74 2.90	.51240 .60617	-.15940	-2.158	.032
Reliability of Computer Software	Bachelor/ High Diploma Master/PhD	98 154	2.68 2.76	.50458 .61798	.07814	1.049	.295

The Bachelor/High Diploma have the highest Mean value of (M = 3.21; SD = .53909), and the education level of Master/PhD have the lowest value of (M = 3.20; SD =.55815). Of all the dimensions only internet security vulnerabilities was found to have statistically significant differences with the educational level of the parents (p<0.05).

CHAPTER 5

CONCLUSION AND RECOMMENDATIONS

This chapter shows a summary of the results of the analyzed data of the study, conclusion and recommendations for future researches.

5.1 Conclusion

To conclude, the study has investigated the awareness of parents towards the safe use of the internet. In this research, a questionnaire sample method was applied for the study. The results showed that parents have a good awareness on all dimensions of the questionnaire. Also, the study showed that parents use Wi-Fi and 3G to access internet connection, and the most important devices frequently used to get online access are mobile phones, laptops computers, tablets, and desktop computers.

It was discovered that there are no statistically significant differences between relative relation of parents on dimensions of the Essential Measures of Online Security, Protect Information Privacy on Websites, Internet Security Vulnerabilities, and the Reliability of Computer Security Software. However, the results showed that there are statistically significant differences between age groups and dimensions of essential measures of online security and reliability of computer security software. But that there are no statistically significant difference between Age groups and variables of protecting information privacy on websites and internet security vulnerabilities. Also, the results have indicated that there are no statistically significant differences between Education level groups on dimensions of essential measures of online security, protect information privacy on websites and reliability of computer security software dimensions, it shows that there are statistically significant difference on the internet security vulnerabilities dimension. Furthermore, the results have indicated that the parents have higher mean scores in the factor of protecting information privacy on websites, and the lowest mean scores were on the factor of reliability of computer security software.

5.2 Recommendations

The results of the study will help parents, educational institutions, organizations as well as of other bodies to enhance the safe use of the internet by children. Future research should focus on parents’ knowledge of using internet filtering software on their children’ computers. This study also shows that parents’ children parents have less awareness of online safety tips, for that reason future studies should concentrate on children’ consciousness and knowledge of safety tips on the internet. In addition, future studies can apply the methodology used in this research in to various geographical settings so as to increase the awareness of parents towards the safe use of the internet for their children safety.

.

REFERENCES

Alqahtani, N., Furnell, S., Atkinson, S., & Stengel, I. (2017). Internet risks for child parents’ perceptions and attitude: An investigative study of the Saudi Context. *In Proceeding of 2017Internet Technologies and Applications (ITA)* (pp. 98-103), rexham, UK: IEEE.

Ayaburi, E.W., & Treku, D.N. (2020). Effect of penitence on social media trust and privacy concerns: The case of Facebook. *International Journal of Information Managemen*t,50,171-181

Bahri, L., Carminati, B., & Ferrari, E. (2018). Decentralized privacy preserving services for online social networks. *Online Social Networks and Media*, 6, 18-25.

Bako, R. K., & Tokes, G. E. (2018). Parental Mediation and Romanian Young Children's Digital Practices. *Revista Romana de Sociologie*, 29(1/2), 23-36.

Barth, S., de Jong, M. D., Junger, M., Hartel, P. H., & Roppelt, J. C. (2019). Putting the privacy paradox to the test: Online privacy and security behaviors among users with technical knowledge, privacy awareness, and financial resources. *Telematics and informatics*, 41, 55-69.

Buch, R., Ganda, D., Kalola, P., & Borad, N. (2017). World of cyber security and cybercrime. *Recent Trends in Programming Languages*, 4(2), 18–23p.

Cavus, N., & Ercag, E. (2016). The scale for the self-efficacy and perceptions in the safe use of the Internet for teachers: The validity and reliability studies. *British Journal of Educational Technology*, 47(1), 76-90.

Cavus, N., & Mohammed, A. A. (2017). Scale for efficacy in the safe use of the Internet for students. *New Trends and Issues Proceedings on Humanities and Social Sciences*, 3(3), 227-234.

Chen, H., Beaudoin, C.E., & Hong, T. (2017). Securing online privacy: An empirical test on Internet scam victimization, online privacy concerns, and privacy protection behaviors. *Computers in Human Behavior*, 70, 291-302.

Chetty, N., & Alathur, S. (2018). Hate speech review in the context of online social networks. *Aggression and violent behavior*, 40, 108-118.

Cohen-Almagor, R. (2018). Social responsibility on the internet: Addressing the challenge of cyberbullying. *Aggression and violent behavior*, 39, 42-52.

Correia, J., & Compeau, D. (2017). Information privacy awareness (IPA): a review of the use, definition and measurement of IPA. *In Proceedings of the 50th Hawaii International Conference on System Sciences*. Hawaii International Conference on System Sciences (HICSS).

Gleason, B., & Von Gillern, S. (2018). Digital Citizenship with social media: Participatory practices of teaching and learning in secondary education. *Journal of EducationalTechnology & Society,* 21(1), 200-212.

Gogus, A., & Saygın, Y. (2019). Privacy perception and information technology utilization of high school students. *Heliyon*, 5(5), e01614.

Grammatikis, P.I.R., Sarigiannidis, P.G., & Moscholios, I.D. (2018). Securing the internet of things: Challenges, threats and solutions. *Internet of Things*,5,41–70.

Heravi, A., Mubarak, S., & Choo, K. K. R. (2018). Information privacy in online social networks: Uses and gratification perspective. *Computers in Human Behavior*, 84, 441-459.

Jeong, Y., & Kim, Y. (2017). Privacy concerns on social networking sites: Interplay among posting types, content, and audiences. *Computers in Human Behavior*, 69,302-310.

Kayes, I., & Iamnitchi, A . (2017). Privacy and security in online social networks: A survey. *Online Social Networks and Media*, 3, 1-21.

Kumar, P. R., Raj, P. H., & Jelciana, P. (2018). Exploring data security issues and solutions in cloud computing. *Procedia Computer Science*, 125, 691-697.

Kusyanti, A., Puspitasari, D. R., Catherina, H. P. A., & Sari, Y. A. L. (2017). Information privacy concerns on teens as Facebook users in Indonesia. *Procedia Computer Science*,124, 632-638.

Lee, H., Wong, S.F., Oh, J., & Chang, Y. (2019). Information privacy concerns and demographic characteristics: Data from a Korean media panel survey. *Government Information Quarterly*, 36(2), 294-303.

Mirza, M. B., Arslan, M., Bokhari, S. T. F., Zafar, R., & Raza, M. (2014). Malicious software detection, protection & recovery methods. *BRIS Journal of Adv. S & T,* (5):PP.14-23

Namanya, A. P., Cullen, A., Awan, I. U., & Disso, J. P. (2018). The world of malware: An Overview. *In Proceedings of 2018 IEEE 6th International Conference on Future Internet of Things and Cloud (FiCloud)* (pp. 420-427). IEEE.

Nouh, M., Nurse, J. R., Webb, H., & Goldsmith, M. (2019). Cybercrime investigators are users too! understanding the socio-technical challenges faced by law enforcement. *In Proceedings of the 2019 Workshop on Usable Security (USEC) at Network and Distributed System Security Symposium (NDSS)*. San Diego, CA, USA: arXiv.

Ogutcu, G., Testik, O. M., & Chouseinoglou, O. (2016). Analysis of personal information security behavior and awareness. *Computers & Security*, 56, 83-93.

Ozdamli, F., & Ercag, E. (2019). Knowledge levels and attitudes toward cybercrimes of adolescents in Northern Cyprus. *TEM Journal*, 8 , 1345-1350.

Parsons, K., Butavicius, M., Delfabbro, P., & Lillie, M. (2019). Redicting susceptibility to social influence in phishing emails. *International Journal of Human-Computer Studies*, 128, 17-26.

Prasad, K. M., Reddy, A. R. M., & Rao, K. V. (2014). DoS and DDoS attacks: defense, detection and traceback mechanisms-a survey. *Global Journal of Computer Science and Technology*, 0975-4172

Shin, W., & Kang, H. (2016). Adolescents' privacy concerns and information disclosure online: The role of parents and the internet. *Computers in Human Behavior*, 54, 114-123.

Somani, G., Gaur, M. S., Sanghi, D., Conti, M., & Buyya, R. (2017). DDoS attacks in cloud computing: Issues, taxonomy, and future directions. *Computer Communications*, 107, 30-48.

Tasril, V., Ginting, M. B., Mardiana, A. P. U. S., & Siahaan, A. P. U. (2017). Threats of computer system and its prevention. *International Journal of Scientific Research in Science and Technology*, 3(6),448-451.

Van Driel, W. D., Schuld, M., Wijgers, R., & van Kooten, W. E. J. (2014). Software reliability and its interaction with hardware reliability. *In Proceedings of 15th International Conference on Thermal, Mechanical and Mulit-Physics Simulation and Experiments in Microelectronics and Microsystems* (pp. 1-8). Ghent, Belgium: IEEE.

Van Schaik, P., Jansen, J., Onibokun, J., Camp, J., & Kusev, P. (2018). Security and privacy in online social networking: Risk perceptions and precautionary behaviour. *Computers in Human Behavior*, 78, 283-297.

Xu, L., Bao, T., Zhu, L., & Zhang, Y. (2018). Trust-based privacy-preserving photo sharing in online social networks. *IEEE Transactions on Multimedia*, 21(3), 591-602.

Yang, X., Jabeen, G., Luo, P., Zhu, X. L., & Liu, M. H. (2018). A unified measurement solution of software trustworthiness based on social-to-software framework. *Journal of Computer Science and Technology,* 33(3), 603-620.

Yang, X., Zhu, L., Chen, Q., Song, P., & Wang, Z. (2016). Parent marital conflict and internet addiction among Chinese college students: The mediating role of father-child, mother-child, and peer attachment. *Computers in Human Behavio*r,59, 221-229.

Yun, H., Lee, G., & Kim, D. J. (2019). A chronological review of empirical research on personal information privacy concerns: An analysis of contexts and research constructs. *Information & Management*, 56(4), 570-601.

APPENDICES

APPENDIX 1

THE AWARENESS OF PARENTS TOWARDS THE SAFE USE OF THE INTERNET

The aim of this questionnaire is to determine the awareness of parents towards the safe use of the internet among parents about internet security to raise the level of awareness of people by online threats while surfing on the internet. Information of this study will be used for academic research only, and all the data you provide in this survey will be protected and not shared with a third party.

Khairi Ghet Elghadafi Elgharnah

Assoc. Prof. Dr. Fezile ÖZDAMLI

Email: 20175720@std.neu.edu.tr

Section 1: Demographic Information.

1- Relative Relation. A. Father □

B. Mother □

C. Other: ------------------- (Please Indicate)

2- Age. ------------ (Please Indicate)

Student Age ---------- How many children do you have --------------

3- Education Level.

A. Bachelor / High Diploma □ B. Master□ C. PhD□

4- How do you access the internet connection?

A. Dial-up□ B. Cable□ C. ADSL□ D. 3G and 4G□ E. Wifi □

F. Other ………… .

5- Which of these devices you use to get online.

A. Desktop Computers □ B. Laptop Computers □

C. Mobile Phones □ D. Tablets □

Section 2: The knowledge questions.

1. Do you know your children's online passwords?

a. Yes □ b. No □

2. Do you know how many hours a week your child spends 'chatting' online with others?

a. Yes □ b. No □

3. Do you use Internet filtering software on all computers your child has access to?

a. Yes □ b. No □

If the answer is yes please indicate the name of software____________________

4. Do you have an 'online rules' agreement with your child?

a. Yes □ b. No □

5. Is the computer your child uses kept in a high traffic area in your home?

a. Yes □ b. No □

6. Does your child know of the safety tips?

a. Yes □ b. No □

Section 3: Awareness of internet security (Please tick in the box of the columns to see your knowledge of internet security).

Items	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
Part 1: Essential Measures of Online Security.					
1-I am conscious of the importance of online internet security software.					
2- I am aware of the riskiness malicious software attacks.					
3- I am conscious of purchasing internet security software from trusted online websites.					
4- I do not concern to share my account password with my friends and family on social media.					
5- I am aware that some of the Internet Security Software contains malware programs.					
6- I am not careful to install any internet security software of any resources on the internet.					
7- I am aware of the cybercrime attacks that threats people's data on the internet.					
8- I have not been learned of keeping personal information secret over the internet.					
9- I am aware to be able to share legal information with trust people on the internet.					
10- I use a unique username and password for all my accounts on social networking.					
11- I am aware of Microsoft recommendations for creating a strong password.					
12- I do not respond to any mysterious requests from a stranger friend on social media.					
13- I know it is difficult, to be honest with anyone on online chatting.					
Part 2: Protect Information Privacy on Websites.					
14-I am aware of applying information privacy policies on social networking against phishing sites.					
15- I know I should not fill out sensitive data of my profile account on social networking.					
16- I Make a complex, unique password and change it every 90 days.					
17- I am careful about what I share on social media with others.					
18- I am careful to avoid posting controversial information on social media.					
19- I am aware that unknown emails addresses may include malware links.					

20- I am not conscious of phishing emails used to convince the victims to send sensitive information.					
21- I do not care about leaving my confidential information exposed to be shared on social sites.					
22- I used to enable and strict privacy settings on social media and websites.					
23- I run the firewall on and update antivirus software while I am surfing online.					
24- I have never click on malicious links that are able to infect my social account.					
25- I am aware of the responsibility for online communication and activities through posting and sharing on chat rooms and emails.					
26- I make online shopping and purchase from secure sites.					
27- I am not able to teach my children how to use the filtering, privacy and safety settings on websites.					
28- I will not share and comment on any person or website spread pornographic materials on social sites.					
Part 3: Internet Security Vulnerabilities.					
29- I have replied to a link that I received on an email and I sent my user account credentials.					
30-My computer system has stopped working by a denial-of-service attack.					
31- I use a username and strong password to login on my computer system.					
32- Using security software tools and services for transferring large data over the internet.					
33- I use internet security programs against architectural weaknesses of the computer system.					
34- I am unaware of using the firewall to control inbound and outbound of internet traffic.					
35- I lost sensitive data without my early knowledge.					
36- My files have been encrypted by malicious ransomware programs.					
37- Implementing anti-spyware software against Internet threats.					
38- I have clicked on a download link and I realized it installed a malware.					
39- I use anti-malware software, ad-blockers and apply safety settings filters to deny access to undesirable content on websites.					
40- I am concerned when I click by mistake on a questionable advertisement on a website page.					
Part 4: The Reliability of Computer Security Software.					
41- Use the latest version of the Anti-virus software and ensure it up to date.					
42- Implementing anti-spyware software against Internet Security threats on the computer system.					
43- Computer system shows a message attack of a malware software "Your machine is not affected".					

44- I make Regularly backup data to be protected from viruses, worms, ransomware, spyware, and Trojan.					
45- I make a backup of sensitive information to be saved in a safe place.					
46- I am not aware of using the reliability and quality of security software on computer.					
47- My files and documents were damaged because of some programs contain Computer viruses and worms.					
48- My computer programs are illegal as it downloaded from untrusted websites.					
49- My computer files were exposed to ransomware software attacks.					
50- I make back up data for an emergency case of malware attacks.					
51- I am aware to use highly efficient and reliability of internet security software.					
52- I am unaware that some of the security software I installed on my computer contains malware and spyware.					
53- I use software to prevent my child to access unsuitable websites.					

Thanks for your contributions to fill this questionnaire.

APPENDIX 2

ETHICAL APPROVAL LETTER

YAKIN DOĞU ÜNİVERSİTESİ

BİLİMSEL ARAŞTIRMALAR ETİK KURULU

30.05.2019

Dear Khairi Ghet Elghadafi Elgharnah

Your application titled **“The Awareness and Perceptions of Parents Towards the Safe Use of the Internet”** with the application number YDÜ/FB/2019/64 has been evaluated by the Scientific Research Ethics Committee and granted approval. You can start your research on the condition that you will abide by the information provided in your application form.

Assoc. Prof. Dr. Direnç Kanol

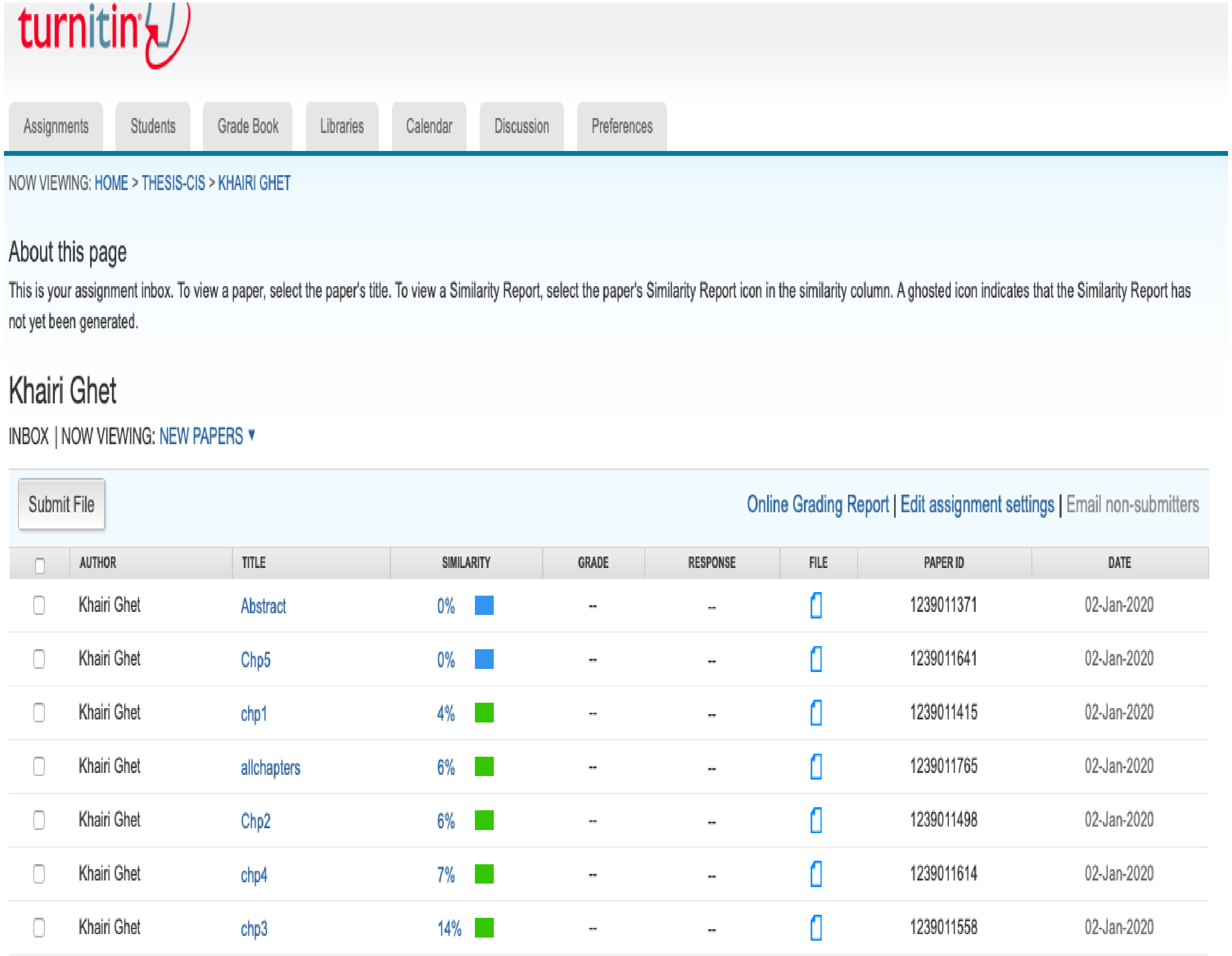
Rapporteur of the Scientific Research Ethics Committee

Direnc Kanol

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

APPENDIX 3

SIMILARITY REPORT



NOW VIEWING: HOME > THESIS-CIS > KHAIRI GHET

About this page

This is your assignment inbox. To view a paper, select the paper's title. To view a Similarity Report, select the paper's Similarity Report icon in the similarity column. A ghosted icon indicates that the Similarity Report has not yet been generated.

Khairi Ghet

INBOX | NOW VIEWING: NEW PAPERS ▾

Submit File
Online Grading Report | Edit assignment settings | Email non-submitters

□	AUTHOR	TITLE	SIMILARITY	GRADE	RESPONSE	FILE	PAPER ID	DATE
□	Khairi Ghet	Abstract	0% 🟦	--	--	🗋	1239011371	02-Jan-2020
□	Khairi Ghet	Chp5	0% 🟦	--	--	🗋	1239011641	02-Jan-2020
□	Khairi Ghet	chp1	4% 🟩	--	--	🗋	1239011415	02-Jan-2020
□	Khairi Ghet	allchapters	6% 🟩	--	--	🗋	1239011765	02-Jan-2020
□	Khairi Ghet	Chp2	6% 🟩	--	--	🗋	1239011498	02-Jan-2020
□	Khairi Ghet	chp4	7% 🟩	--	--	🗋	1239011614	02-Jan-2020
□	Khairi Ghet	chp3	14% 🟩	--	--	🗋	1239011558	02-Jan-2020