INVESTIGATING UNIVERSITY STUDENTS' PERCEPTIONS ON THE SAFE USE OF COMPUTER AND THE INTERNET SECURITY: A CASE STUDY IN NORTH PART OF IRAQ

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

By

DIDAR DLSHAD HAMAD AMEEN

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

NICOSIA, 2015

DIDAR DLSHAD INVESTIGATING UNIVERSITY STUDENTS' PERCEPTIONS ON THE SAFE USE OF NEU
HAMAD AMEEN COMPUTER AND THE INTERNETSECURITY: A CASE STUDY IN NORTH PART OF IRAQ 2015

INVESTIGATING UNIVERSITY STUDENTS' PERCEPTIONS ON THE SAFE USE OF COMPUTER AND THE INTERNET SECURITY: A CASE STUDY IN NORTH PART OF IRAQ

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

By
DIDAR DLSHAD HAMAD AMEEN

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

NICOSIA, 2015

Didar Dlshad HAMAD AMEEN: INVESTIGATING UNIVERSITY STUDENTS' PERCEPTIONS ON THE SAFE USE OF COMPUTER AND THE INTERNET SECURITY: A CASE STUDY IN NORTH PART OF IRAQ

Approval of Director of Graduate School of

Applied Sciences

Prof. Dr. İlkay SALİHOĞLU

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

Examining Committee in Charge:

Prof. Dr. Dogan Ibrahim	Committee Chairmen, Computer Information Systems Department, NEU
Assoc. Prof. Dr. Nadire Cavuş	Supervisor, Computer Information Systems Department, NEU
Assist. Prof. Dr. Seren Başaran	Committee Member, Computer Information Systems Department, NEU
Assist. Prof. Dr. Ümit İlhan	Committee Member, Computer Engineering Department, NEU
Assist. Prof. Dr. Müesser Nat	Committee Member, Management Information Systems Department, CIU

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: Didar Dlshad Hamad Ameen

Signature:

Date:

ACKNOWLEDGEMENTS

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

I would like to thank Prof. Dr. Dogan Ibrahim and Assist. Prof. Dr. Seren Başaran who have been very helpful through the duration of my thesis, this thesis could not have been achieved without their generous and professional assistance.

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

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

To my parents...

ABSTRACT

Day by day the number of the students who are using Internet is increasing, and this affects the student negatively. Hence this research is aimed to investigate the self-efficacy and personal computer user's perception towards Computer and Internet security amongst University Students in North part of Iraq. Research based model and questionnaire was used in the study where data are collectedrandomly from 709 students, and the volunteered have been chosen from Faculties of Arts and Engineering in Soran University, Salahaddin University and University of Sulaimani during 2014-2015 Spring semester. The dependent variables in the study are Social Networking Sites (SNS), Malicious Software (MS), Web Security & Social Engineering (WSS), and Computer Security (CS). SPSS was used to analyze the data; one-way ANOVA and independent *t*-test were used to compare variables. After statistical analysis of collected data the results improved that most of the students 37.9% spend about 4-5 hours daily, 42.3% use the Internet for social media purposes and 85% of the students do have antivirus on their computer. It was also found that there are significant differences in the overall to security awareness system between the demographic information such as gender, age and faculty.

Keywords:Computer security;Internet security;malicious software; social network sites; student perceptions

ÖZET

Gün geçtikçe Internet kullanan öğrencilerin sayısı artıyor ve bu da olumsuz öğrenciyi etkilemektedir. Dolayısıyla bu araştırma Irak'ın kuzey kesiminde Üniversite Öğrencileri arasında öz yeterliliği ve Bilgisayar doğru kişisel bilgisayar kullanıcısının algı ve İnternet güvenliği araştırılması amaçlanmıştır. Araştırma temelli bir model ve anket verileri rastgele olduğunu ve gönüllülük ilkesi sırasında Irak'ın kuzey kesiminde Sanat ve Mühendislik Fakültesi Süleymaniye'deki arasında Soran Üniversitesi Selahaddin Üniversitesi ve University seçildi 709 öğrenciden toplanan çalışmada kullanılan 2014-2015 Bahar dönemi. Çalışmada bağımlı değişkenler Sosyal Ağ Siteleri (SNS), Kötü Amaçlı Yazılımları (MS), Web Güvenlik & Sosyal Mühendislik (WSS) ve Bilgisayar Güvenliği (CS) bulunmaktadır. SPSS verileri analiz etmek için kullanılır; tek yönlü ANOVA ve bağımsız t-testi değişkenlerin karşılaştırılmasında kullanıldı. Toplanan verilerin istatistiksel analizi sonrasında sonuçları öğrencilerin% 37.9 çoğu yaklaşık 4-5 saat, günlük ve% 42.3 harcamak sosyal medya amaçlı Internet kullanımı ve öğrencilerin% 85'i kendi bilgisayarında antivirüs var olduğunu düzeldi. Aynı zamanda cinsiyet, yaş ve öğretim gibi demografik bilgiler arasında güvenlik bilinci sistemine genel olarak önemli farklılıklar olduğu tespit edilmiştir.

Anahtar Kelimeler: Bilgisayar güvenliği;Internet güvenliği;Kötü amaçlı yazılım; Sosyal ağ siteleri; Öğrenci algıları

TABLE OF CONTENTS

CHAPTER 1: INTRODUCTION

CHAPTER 2: RELATED RESEARCH

CHAPTER 3: THEORETICAL FRAMEWORK

CHAPTER 4: METHODOLOGY

CHAPTER 5: RESULTS AND DISSCUSSION

CHAPTER 6: CONCLUSION AND RECOMMENDATIONS

APPENDICES

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATION

ANNOVA:	Analysis of Variance
CS:	Computer Security
CSE:	Computer Self-Efficacy
FOA:	Faculty of Arts
FOE:	Faculty of Engineering
IT:	Information Technology
LAN:	Local Area Networks
MS:	Malicious Software
PC:	Personal Computer
PSP:	Perceived Security Protection
RAM:	Random Access Memory
SD:	Standard Deviation
SNS:	Social Networking Sites
WAN:	Wide Area Networks
WSS:	Web Security & Social Networking Sites

CHAPTER 1
INTRODUCTION

It is important to protect information within computer systems because most organization solely depends on computer systems for the collection, processing and information storage (Ng and Rahim, 2010). A PC security episode is characterized as a security-related unfriendly occasion in which there is lost data privacy, interruption of data or framework uprightness, disturbance or disavowal of framework accessibility, or infringement of any PC security strategies. As per the 2007 yearly review directed by the Computer Security Institute, 46% of respondents demonstrated that their association encountered a security episode inside of the most recent 12 months. Of these, a noteworthy number (52%) of the assaults are infection related. It is thusly imperative for associations and representatives to know about and ensure themselves against security dangers and cybercrime. Nations around the globe have made laws (e.g., Computer Misuse Act in Britain and Singapore) and set up national offices (e.g., the Computer Analysis Response Team in the US) to battle PC security dangers. Different advances are connected at the national level for this reason, for example, a PC reconnaissance framework created by the FBI. Further, hierarchical measures are vital in this battle. Associations need to create and execute a multidimensional way to deal with protection their data resources. Among the methodologies, innovative measures, for example, firewalls for border safeguard are basic in associations. Such arrangements are fundamental however not adequate for security (Boon-Yuen and Azree, 2010).

The issues of PC security can, to a sure degree, be alleviated by innovation based arrangements, for example, cryptography and verification components. On the other hand, PC security is not only a specialized issue. The achievement of security likewise relies on upon the viable conduct of clients. The human element has over and again been said to be the weakest join in PC security. It is hence important to consider the socio-behavioral viewpoint and investigate the components that impact a client's expectation to practice home PC security. A more extensive vision that addresses social gatherings and conduct is required. The catalyst for our study is the way that next to no has been done to examine the behavioral parts of home PC clients, as for PC security (Hsiao et al., 2012). This is on account of achievement of PC security relies on upon the viable conduct of clients. Workers in an association assume a vital part in the aversion and location of security episodes. While framework chairmen are in charge of designing firewalls and servers in a safe way, clients are in charge of rehearsing security countermeasures, for example, picking and ensuring proper passwords. In this way, for powerful security, clients need to settle on a cognizant choice to follow the association's security approaches and embrace PC security conduct. To this end, associations have been actualizing security preparing and mindfulness projects to teach clients (Ng and Rahim, 2010). While numerous specialist rules are accessible, there is an absence of observational studies concerning the configuration and viability of security mindfulness programs. A successful mindfulness system ought to impact a client's demeanor and conduct to be more security-cognizant. Accordingly, it is basic to comprehend what will impact a client's security conduct so that fitting mindfulness projects can be outlined. Notwithstanding, there is little hypothetically grounded observational data frameworks research on the conduct of people in rehearsing secure figuring.

As indicated by Carruth and Ginsberg (2014) self-efficacy recognitions about one's PC use, Internet and SNS abilities may be another variable identified with individual contrasts in desires of individual control of PC security. Bandura (1997) characterized self-efficacy as people groups' convictions about their abilities to create assigned levels of execution that practice impact over occasions that influence their lives. Convictions about self-efficacy decide how individuals feel, think, inspire themselves and carry on. Disappointment is owing to an absence of exertion or learning of aptitudes. Testing undertakings are met with certainty. Interestingly, individuals with a powerless feeling of self-efficacy perspective difficulties as dangers that ought to be maintained a strategic distance from. On the off chance that they are confronted with troublesome errands, they concentrate on their inadequacies and potential unfriendly impacts as opposed to the assignment, which makes them waver and surrender rapidly (Carruth and Ginsberg, 2014). Singular contrasts in convictions about self-efficacy can be created by four wellsprings of impact: dominance encounters, vicarious encounters, social influence, and enthusiastic states. The best approach to pick up a feeling of self-efficacy is by authority experience. Achievement reinforces a man's self-efficacy, while disappointment undermines it. A genuine feeling of self-efficacy is obtained when one overcomes deterrents with diligence and flexibility, and can achieve their objective. Vicarious encounters are another method for fortifying one's self-efficacy. Using so as to watch individuals that are like you succeed diligent work and devotion raises one's conviction of being fit for mastering comparable strategies. Social influence can likewise be a compelling method for raising a man's self-efficacy. On the off chance that they are verbally empowered and convinced that they can succeed, it is more probable that they will advance more exertion and maintain that push to succeed. Individuals' passionate states likewise affect their capacity to succeed. They may liken stretch or weakness with indications of disappointment or defenselessness. Individuals' state of mind, whether constructive or pessimistic, can likewise affect a man's self-efficacy. These elements can assume a key part in the improvement of a man's self-efficacy (Carruth and Ginsberg, 2014). Past examination on PC self-efficacy demonstrated that PC experience had a huge positive relationship on PC self-efficacy convictions (Hsiao et al., 2012). PC self-efficacy alludes to individual self-efficacy about utilizing PCs, and has been recognized as a noteworthy determinant of PC related capacity and use in hierarchical settings (Madhavan and Phillips, 2010). Be that as it may, a few past studies have analyzed variables influencing PC self-efficacy convictions (Madhavan and Phillips, 2010; Hsiao et al., 2012; Carruth and Ginsberg, 2014). PC self-efficacy may decide the accomplishment of PC learning. At the end of the day, the social intellectual hypothesis gives a strong hypothetical establishment to the idea of PC self-efficacy. In different studies, PC self-efficacy has a noteworthy positive association with improved higher execution, and expanded PC utilization (Hsiao et al., 2012). Sam et al. (2005) has recommended that self-efficacy may be a vital variable identified with the obtaining of figuring aptitudes. PC self-efficacy is a particular sort of self-efficacy. Particular self-efficacy is characterized as confidence in one's capacity to prepare the inspiration, intellectual assets, and strategies expected to meet given situational requests. Along these lines, PC self-efficacy is a conviction of one's capacity to utilize the PC and members with little trust in their capacity to utilize PCs may perform all the more ineffectively on PC based errands. Then again, past PC experience may persuade PC applications courses are simple (Sam et al., 2005). PC Self-Efficacy has been appeared to affect classroom execution accordingly the precursors to Computer Self-Efficacy (CSE) may give an instrument that can be utilized to impact it. Various predecessors and consequents of PC self-efficacy have been examined.

Hauser et al. (2012) bunch these forerunners into classifications, for example, social impact (consolation, administration bolster), demographic variables (experience, age, sex, earlier execution), and convictions (self-originations of capacity, nervousness). So also, results are assembled into results (execution, fulfillment, learning), convictions (influence, nervousness, result desires), and practices (use, early appropriation). Regularly Computer Self-Efficacy is utilized as a part of the general feeling of utilizing a PC to achieve a huge number of undertakings. A typical measure for the reliant variable is essentially PC use or the recurrence of utilizing a PC. PC Self-Efficacy was initially conceptualized in the connection of general assignment execution utilizing a PC. PC Self-Efficacy has additionally been incorporated into late studies in connection to application-particular assignments (Hauser et al., 2012). General Computer Self-Efficacy alludes to a conviction that the subject can perform well over an assortment of PC assignments. Particular Computer Self-Efficacy alludes to the conviction that the subject can perform well utilizing a specific innovation, for example, programming, database advancement, and so on. Be that as it may, where the subject’s involvement with a PC is not to a great degree high, just like the case with a considerable lot of the subjects in this study, particular Computer Self-Efficacy clarifies more change concerning anticipating execution of the assignment than general Computer Self-Efficacy (Hauser et al., 2012).

1.1 The Problem

PC client is frequently said to be the weakest join in PC security. Security and protection dangers, for example, Web cookies and phishing require some type of client complicity or passive consent. Sufficient security does not accompany the buy of the PC but rather requires extra programming watchful settings inside of utilizations, suitable decisions of passwords, standard overhauling of patches, and so forth. Additionally, as applications are turning out to be all the more fascinating/helpful and organizations are moving far from paper, home PC clients are performing more delicate undertakings online and putting away more private information on their PCs. Episodic proof, overviews, and studies figure out that home PC clients frequently don’t sufficiently comprehend the dangers, or have room schedule-wise, longing and information to have the capacity to handle them. As substantial episodes of worms and infections have appeared, even frameworks managers are not sufficiently industrious in applying patches to enhance security (Kin and Bauer, 2010). From the various literatures surveyed it was found out there are little or no work has been done on students' perception on Internet and computer security in North part of Iraq. So this study is the breach the gap in this area of research in the country.

1.2 The Significance of the Study

College understudies are overwhelming clients of the Internet contrasted with the overall public, and they assume a pivotal part in securing the Internet, and assurance of PCs is left to the activity of the clients (Ayub et al., 2014). The harm because of PC security occurrences is persuading understudies to receive defensive components. While innovative controls are vital, PC security likewise relies on upon singular's security conduct. It is along these lines critical to explore what impacts understudies to practice PC security which will help the students, parents and most probably the government or universities to know the possible weakness of students' knowledge of computer security problems and help propose a possible solution that will help salvage this problem.

1.3 The Aim of the Study

The main aim of the study is to investigate self-efficacy and students' perception towards computer and the Internet security amongst University students in North part of Iraq. In order to achieve this aim the answers to the following questions were sought:

1. What are the students' self-efficacy and perceptions in the use of computer and Internet security?
    1.1. What are the students' self-efficacy and perceptions in the use of computer and Internet security based on Security on Social Networking Sites?
    1.2. What are the students' self-efficacy and perceptions in the use of computer and Internet security based on Malicious Software?
    1.3. What are the students' self-efficacy and perceptions in the use of computer and Internet security based on Web Security and Social Engineering?

1.4. What are the students' self-efficacy and perceptions in the use of computer and Internet security based on Computer Security?

2. Is there any gender based difference on students' self-efficacy and perceptions in the use of computer and Internet security?

   2.1. Is there any gender based difference on Security on Social Networking Sites?

   2.2. Is there any gender based difference on Malicious Software?

   2.3. Is there any gender based difference on Web Security and Social Engineering?

   2.4. Is there any gender based difference on Computer Security?

3. Is there any age based difference on students' self-efficacy and perceptions in the use of computer and Internet security?

   3.1. Is there any age based difference on Security on Social Networking Sites?

   3.2. Is there any age based difference on Malicious Software?

   3.3. Is there any age based difference on Web Security and Social Engineering?

   3.4. Is there any age based difference on Computer Security?

4. Is there any faculty based difference students' self-efficacy and perceptions in the use of computer and Internet security?

   4.1. Is there any faculty based difference on Security on Social Networking Sites?

   4.2. Is there any faculty based difference on Malicious Software?

   4.3. Is there any faculty based difference on Security and Social Engineering?

   4.4. Is there any faculty based difference on Computer Security?

5. What is the age, gender, and faculty based differences with respect perception towards computer and Internet security in total?

   5.1. Is there any age based difference on the total average score?

   5.2. Is there any gender based difference on the total average score?

   5.3. Is there any faculty based difference on the total average score?

1.4 Limitations of the Study

The limitations of the study:

- This study was only limited for university students, as it was applied on undergraduate and postgraduate (Master's and PhD) students.
- Due to the large data required three universities were used for this study.

- Time of the study was a major limitation in the sense that if this study will be carried out again at the future, the perceptions of the students will be changed towards computer and Internet security.

1.5 Overview of the Thesis

Chapter 1: Give details about the general introduction of computer and the Internet security, the problem definition, the significance of the study, the aim of study, the limitation of this study and most importantly the breakdown of this study.

Chapter 2: Presents the related research work on computer security, computer self-efficacy, web security, social networking sites and malicious software.

Chapter 3: Introduces the theoretical framework whereby various aspects of computer and Internet security, malicious software etc. were discussed.

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

Chapter 5: The results and discussion were discussed in details.

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

CHAPTER 2
RELATED RESEARCH

2.1 Computer Security

Gercke (2012) proclaimed that upgrading web security and defensive urgent information foundations are fundamental to each country’s security and monetary prosperity. Making the web more secure (and defensive web clients) has gotten to be fundamental to the occasion of late administrations also as government strategy. Hindering law-breaking is a necessary component of a national digital security and requesting information framework insurance system. In particular, this incorporates the reception of material enactment against the abuse of ICTs for criminal or distinctive capacities and exercises expected to affect the trustworthiness of national vital frameworks. At the national level, this can be a mutual obligation requiring composed activity connected with bar, arrangement, reaction and recuperation from occurrences with respect to government powers, the individual part and voters. At the local and global level, this involves participation and coordination with significant accomplices.

As indicated by Aboud (2012) the definition and usage of a national system and methodology for digital security so needs a far reaching methodology. Digital security strategies – for example, the occasion of specialized assurance frameworks or the instruction of clients to prevent them from changing into casualties of law-breaking – will encourage scaling back the possibility of law-breaking. The occasion and backing of digital security techniques are a noteworthy part inside of the battle against law-breaking. The lawful, specialized and institutional difficulties uncover by the issue of digital security are world and much coming to, and might singularly be tended to through a lucid methodology contemplating the part of different partners and existing activities inside a system of universal participation. Aboud conjointly portray the law-breaking as a culpability abuse an information association as a way through that it’s drilled.

2.1.1 Online privacy and security

Citron (2010) demonstrated that in light of the fact that the web is changing into an essential a part of individuals' lives, extra enterprises utilize the web for business. This came about with the transmission of gigantic measures of learning wherever the ability for putting away, recovering and recognition data obviously rises. Clearly, web has 2 very surprising confronts one grants energizing open doors for individuals to figure, organize and unravel their ideas on-line. Alternate makes individuals helpless and keeps them from working together similarly in on-line setting.

Mikovce and Hutinski (2010) pronounced that on-line clients' conduct is affected by the exchange offs between what one gives up (like uncovering of some sensibly data) and what one additions from it (advantages like day in and day out openness of administration, efficient or distinctive accommodations). Then, hyperbolic danger in on-line outcomes is at present perceived in a major choice of dangers that get to explicitly focus on-line clients and endeavor information with respect to them.

Belanger et al. (2010) has researched the significance of 4 trust files that impact web clients buy aim and attitude to supply individual information. The encased trust records were: (1) outsider protection seal, (2) security explanation, (3) outsider security seal, and (4) efforts to establish safety. The outcomes demonstrate those respondents' value efforts to establish safety the preeminent.

Wang et al. (2010) explored however saw quality impacts the client's acknowledgment of e-managing an account. Seen quality enveloped 2 measurements: security and protection issues. Security commented level of certification that a chose dealings will be performed with none security break. Security commented insurance from the social event of shifted data all through clients' collaboration with a bank. Consequences of the performed examination demonstrate that apparent quality (e.g. to reason that exchanges are secured and are defensive their protection) had a noteworthy positive effect on clients' conduct aims.

Scott (2010) pointed out sixteen e-business dangers. Inside of the study members were solicited to rate their observations of the sixteen dangers. 3 high issues for two hundred encased members were gainfulness hazard, security danger and protection hazard. The connections between 3 trust concerns (merchant, web and outsiders) and clients' states of mind towards on-line getting were inspected. The creators found that the association between trust in an exceptionally merchant and edge towards on-line getting gets to be extra fundamental once people have higher protection and security issues. Furthermore, they found that once people have higher protection and security issues the association between trust in web and edge towards on-line getting debilitates.

2.2 Computer Self-Efficacy

PC Self-Efficacy refers to one's conviction of their capacity to perform a chose undertaking (Bandura 1997). Bandura pronounced that the primary center isn't on the specific abilities however the judgments one has of what one will do with no make a difference aptitudes one has. individuals Who comprehend themselves fit for performing expressions bound errands or exercises are plot as being high in self-efficacy, and are extra certainly to attempt these assignments and exercises; and contrariwise. Inside of the connection of pc use, pc self-efficacy alludes "to a judgment of one's ability to utilize a PC" (Bandura, 1997).

Teo and Koh (2010) found that a singular's utilization of innovation was experiencing their self-efficacy which members with higher self-efficacy convictions utilized PCs extra ordinarily and toughened less PC related nervousness. The writers conjointly noticed that individuals with higher pc self-efficacy convictions have a tendency to envision themselves as prepared to utilize innovation. Those with lower pc self-efficacy convictions have a tendency to end up extra annoyed and restless once working with PCs; and falter to utilize PCs after they experience impediments. PC self-efficacy envelops a noteworthy effect on Associate in Nursing singular's desires towards abuse pcs and individuals Who didn't consider themselves to be skilled PC clients have a tendency to not utilize PCs.

Studies led by Litterell et al. (2005) observed that PC self-efficacy will build execution and lessens pc incited tension.

Albion (2001) has noticed that instructors' PC self-efficacy may be a key issue determinative their examples of PC use. For pre-administration scholastics, their PC self-efficacy extensively anticipated that their capacity would coordinate innovation use inside of the schoolroom.

Zhao et al. (2002) expressed that PC self-efficacy are regularly seen as application-particular and measured as one's apparent certainty for the different area particular aptitudes with connection to pc use.

Cavus and Ercag (2014) reported from their study on "the scale for the self-efficacy and observations in the protected utilization of the Internet for instructors: The legitimacy and unwavering quality studies" that the scale regarding legitimacy and dependability was observed to be suitable in all parts of the essential criteria. Accordingly, the created scale could offer or some assistance with being utilized by instructors, in Cyprus and in different nations, to have the capacity to get to the Internet securely and help them in other experimental zones of study in deciding educators' self-efficacy.

Murphy et al (1989) made a mainstream measure, the PC self-efficacy scale, was made for movement people's impression of unequivocal PC related information and aptitudes. The 32-thing scale measures 3 levels of figuring abilities: fledgling's level, propelled level, and level identified with centralized server PCs. From that point forward, a few analysts have customized the first Murphy's PC self-efficacy scale while others have custom-made a somewhat changed form of the Murphy scale.

In any case, Abbitt and Klett (2007) reported that an issue confronted with using existing PC self-efficacy scales is that they should supplant things identified with out-dated innovation like PC diskettes andCD-ROM databases.

Lee and Tsai (2010) reported that the multiplication of web 2.0 and media apparatuses for the purpose of education has conjointly made it important to ponder these advances as a part of lectures' PC self-efficacy investigation. Late studies have started to investigate extra particular assortments of pc self-efficacy, e.g. web self-efficacy. Less consideration has been paid on building up a bland pc self-efficacy scale that accompanies fundamental pc abilities, online aptitudes, and abilities with media devices.

Saade and Kira (2009) expressed PC self-efficacy assumes a noteworthy part in intervening the effect of pressure on saw basic use. The extra the laborer fuses with the pc, the extra they feel guaranteed in taking care of the pc at their work. This guideline found by pc self-efficacy is above all else, decreasing the quality and centrality of the effect of strain on saw straightforward utilize the pc and second, having a noteworthy contact with pc tension. A few scientists have focused on the relationship of self-efficacy to assortment of situational variables.

Carroll et al. (2009) considers that self-efficacy trusts seem to anticipate a few instructive results and impressively connected with distinctive inspiration develops and instructive exhibitions.

Furthermore, in accordance with Weng et al. (2009) understudies with high self-efficacy saw disappointment encounters as difficulties rather than dangers inferable from more grounded self-efficacy desires. Later, (Maimunah et al., 2012) supplementary, instructor’s and understudy’s demeanors and self-efficacy discernments with respect to PC upheld training is that the essential issue to acknowledge achievement in pc bolstered instruction rehearses.

In any case, as indicated by Guy and Jackson (2010) upheld the self-efficacy accepts measured by scientists at generally Black personnel or University (HBCU) inside of the South, not all understudies are great with working environment applications.

Abele and Spurk (2009) refered to that their study utilizes self-efficacy, as a site particular live of PC tension inferable from its bigger prophetical control over general and undertaking particular measures. Other than that, self-efficacy conjointly has been reportable by a wide range of analysts to relate completely to figure engagement and laborer prosperity (Xanthopoulou, 2009).

Baronand Morin (2010) presumed that in things wherever honing expects to create administration aptitudes, the measuring of abilities exchange is normally a generous test. Hence, a few scientists have opined for the measuring of self-efficacy in light of the fact that the fundamental result of instructing, and a couple vocation studies have started to attempt to an identical.

Yanik (2010) reported that there are a few studies concerning PC upheld training, impression of pc self-efficacy, pc nervousness and along these lines the mechanical mentalities of scholastics and educator applicants.

Usher and Pajares (2009) expressed that all in all, this study is directed in order to imagine however PC and tension has an impact on representatives' PC self-efficacy. Wellsprings of PC self-efficacy were measured utilizing 24-thing Sources of PC Self-efficacy scale customized from the 24-thing Sources of number-crunching Scale.

Hence, Maimunah et al. (2011) watched that PC self-efficacy are regularly measure using Meta-diagnostic audit, beginning and most clear target is to check speculations. Meta-logical survey will serve 2 pivotal elements of educating observational work on PC self-efficacy: hypothesis testing and hypothesis building.

2.3 Web Security

Baaij (2012) proclaimed that utilization of web is nowadays regular way of life see in modern nations. The vast majority of the general population can't envision an existence while not the ethics and prospects of web. However the fast ascent and pervasive character of web conjointly made a few level headed discussions concerning wellbeing and security issues. With the development of web use, conjointly new dangers and threats went ahead. At present, web security is politically and socially a key issue. One among the courses by which governments endeavor to animate web security, is to create client mindfulness battles. Be that as it may, the adequacy of those crusades is addressed.

Furnell (2010) contend that invigorating client obligation regarding by and large on-line security may be an intriguing and feasible objective. However distinctive studies are more suspicious towards the opportunities to impact client conduct and report that mindfulness raising devices and diverse security devices for completion clients ordinarily need sway.

Mekovce and Hutinski (2010) reportable from their study that individuals generally dither to utilize administrations offered through web owing to their suspicions concerning the measure of offered (1) assurance of their protection and (2) security of performing expressions on-line exchanges. Security is by and large included with the specifiable client data and clients' rights to claim administration over their data. On the inverse hand, security gives the physical, intelligent, and procedural protections that are required to keep with it individual. Protection can't be accomplished while not getting security watch, nor can the utilization of security components ensure insurance of protection. In spite of being firmly joined in watch, protection and security are saw as isolated issues by on-line clients.

Eurostat's data (2010) demonstrates that 35% of respondents (incorporated into investigation in 2010) don't use on-line administrations inferable from their issues concerning security of exchanges, and half-hour of respondents don't use on-line administrations owing to issues connected with protection issues, e.g. loss of non-open data. Along these lines, in order to amplify the net clients' certainty inside of the security of their data, enterprises (online administration suppliers) should have various components that administration access to the keep data.

On the inverse hand, Ye and Zhong (2011) referred to that the shot of on-line clients' loss of administration over their own information should be diminished. On-line clients should have administration (1) over uncovering of their own information to others, furthermore as (2) over future use of the unveiled information.

Saprikis et al. (2010) reportable from their study that the sharp increment of web utilization, and in addition, the efficient advancement of information Technology has rebuilt the strategy item are purchased and oversubscribed, resulting to the exponential development inside of the scope of web purchasers. On the other hand, a lot of varieties worried on-line buys are unconcealed inferable from the fluctuated shoppers' qualities and thusly the assortments of gave stock and administrations. In this manner, comprehension who are those exceptional and why they select to utilize or stay away from the web as a channel may be an imperative issue for every e-trade chiefs and customer scholars. Their examination gives consideration snatching bits of knowledge on the net customer conduct, as their outcomes show imperative varieties between the 2 groups of respondents.

As indicated by Monsuwe et al. (2010), the extension inside of the scope of online customers is bigger than the development in web clients, showing that extra web clients are getting settled to purchase on-line. Notwithstanding that, not exclusively will the measure of adopters become however conjointly the amount of their buys is proportionately expanded.

As per Chen et al. (2014) security is based, to some degree, upon the reasonable comprehension of dangers and in this manner the utilization of systems to alleviate these dangers. Web scenes and in this way the utilization of the web in creating nations are massively entirely unexpected contrasted with those in made nations wherever innovation is extra pervasive. Amid this work, we tend to investigate the usage of web innovation all through urban and peri-urban African country and look at demeanors toward security to quantify the degree to this new populace of innovation clients is likewise inclined to assaults. They see that, as in North America and Europe, the overflowing mental danger model demonstrates a shortage of comprehension of however web advances work (Chen et al., 2014). Subsequently, people accept vigorously upon passwords for security on-line and individuals who enlarge their security do accordingly with a spread of unexpected practices learned by overhearing people's conversations. We tend to relate and refinement our discoveries to past works and make numerous proposals for up security in these connections.

Wash (2010) examined mental models of information processor security in a shot to get a handle on however home clients make security decisions. Information processor frameworks are frail as an aftereffect of their controlled by untrained clients. The increment of botnets has enhanced this issue; aggressors trade off these PCs, blend them, and utilize the following system to assault outsiders. Regardless of a curiously large security exchange that gives bundle and proposal, information processor clients stay helpless. He decide eight "people models" of security dangers that are utilized by information processor clients to settle on a choice what security bundle to utilize, and that educated security suggestion to take after: four conceptualizations of "infections" and distinctive malware, and 4 conceptualizations of "programmers" that burgled PCs. He conjointly outlined however these models are won't to legitimize overlooking learned security proposal. At last, depict one motivation behind why botnets are in this way troublesome to kill: they cleverly advantage of crevices in these models so a few information processor clients don't find a way to shield against them.

Herley’s work investigating client mentalities toward pc security in created nations have unconcealed that people ordinarily comprehend security as baffling boundaries to profitability and at last useless. Dourish and Grinter found that clients by and large delegate security to the innovation itself, distinctive individuals, elements, or associations. He conjointly contends that clients’ dismissal of the security proposal they get is totally discerning from a financial viewpoint (Herley, 2010).

Research from e.g. Lindgaard et al. (2011) and Cyr et al. (2010) plainly exhibits that the characteristic of a web website depends, at least in a few ways that and to some degree, on the system it’s presented to the client and in this manner the client’s impression of its quality and security. Individuals are thinking of WebPages in light of this for at least fifteen years.

2.4 Social Networking Sites

As indicated by Mahajan (2009) the exponential development of the web has made it enter for all intents and purposes every side of the globe, and for a few to affect practically every side of way of life. One among the principal wide utilized web applications over the age compass is that the Social Networking Sites. A Social Networking site may be a part in light of line group wherever clients regularly start by posting essential information in regards to themselves – commented as "Profiles" – then speak with distinctive individuals in an exceptionally kind of ways that and on a spread of points.

Moreover, SNSs give clients with entertainment opportunities like recognition recordings, observing music, tuning in on-line recreations, and scanning the everyday news (Orchard et al., 2014; Shin and Shin, 2011). As a consequence of such a lot of youth have a place with SNSs these destinations can possibly significantly affect the social and mental improvement of youth who use them (e.g., relationship quality and prosperity; Kross et al., 2013; Kuss and Griffiths, 2011; Liu and Yu, 2013; Reinecke and Trepte, 2014). 2 of the extra basic SNSs inside of the U.S. are Facebook and Twitter.

O’Keeffe and Clarke-Pearson (2011) expressed that in China Renren and Qzone are the most informal community destinations utilized. Renren, once alluded to as Xiaonei (inside

University), is that the Social Networking site most all around enjoyed among Chinese youthful grown-ups. Like Facebook, Renren grants clients to make a profile wherever they'll post information with respect to themselves, similar to their staff, organization, occupation, flagging, email location, hobbies, and most loved music. Renren conjointly gives capacities like open and individual electronic correspondence among clients, period moment electronic correspondence, on-line diversions, and video sharing, fundamentally the same to Facebook. Qzone was made by Tencent in 2005. It grants clients to record websites, keep journals, send photographs, hear music, and watch recordings. Clients will set their Qzone foundation and pick embellishments upheld their inclinations so each Qzone is made-to-request to the individual part's style. Be that as it may, most Qzone administrations aren't free; exclusively once looking for the "Canary Diamond" will clients get to every administration while not paying further. Given the enormous scope of SNS clients and accordingly the potential effect of SNS use on social and mental prosperity, it's important to get a handle on the basic component whereby SNS use impacts these results.

The few studies that have examined the system behind the association between SNS use and these social and mental results have made conflicting results (Jelenchick et al., 2013; Liu and Yu, 2013) for case; Jelenchick et al. (2013) analyzed the association between SNS use and discouragement among more established U.S. teenagers and found no relationship. On the other hand, a report by the yankee Academy of prescription encouraged that abuse Facebook could bring about despondency (Kross et al., 2013).

Discoveries of Andreassen et al. (2012) study encouraged that the abuse of SNSs could bring about SNS dependence, however the method for "abuse" amid this setting is vague. In refinement, distinctive studies have reportable a positive relationship in the middle of SNSs and mental prosperity (Kim and Lee, 2011; Valkenburg et al., 2006).

Valkenburg and Peter (2009) expressed that irregularity is likewise attributable to the Catch 22 of the term "over use" and accordingly the bearing of connection of those variables. Will "abuse" of SNSs reason wretchedness or will sadness bring about the "abuse" of SNSs, possibly to escape melancholy? Another danger encouraged by a superior survey of the writing is that the association between abuse of SNSs and melancholy could depend to the sort of SNS utilized.

One special case may be an investigation of the social effect of abuse Facebook (Kim and Lee, 2011). Kim and Lee (2011) found that the measure of Facebook companions and giving a decent representation of oneself to others was totally connected with the client's prosper satisfaction.

2.5 Malicious Software

Shukla et al. (2014) reported that pernicious projects get transmitted into the pc system while not the information of its clients and aren't good with the framework. Once the pc projects are run, the infections get flowed along the edge of the projects and begin tainting related projects that acquire its contacts. There exists a potential risk of distinctive associated frameworks acquiring contaminated as well. Malwares will develop on a system just because of the interconnectivity of workstations. Such develop are frequently hazardous if the PCs have important data which may get undermined by infections as an aftereffect of all hubs inside of the system are in the end tainted. To clean the framework, antivirus bundle is utilized to dispose of infections in tainted system of hubs and safeguard distinctive hubs by diagnostic them, the insurance being administered by bundle with a steady rate that is generally blessing inside of the framework.

Hachman expressed that PC and learning frameworks are unendingly under flame, making outside dangers a decent sympathy toward enterprises. For instance, the Hactivist group "Unknown" as of late oversubscribed the ASCII content document for PCAnywhere as a consequence of Symantec did not pay their payment (Hachman, 2012).

Enrici et al. demonstrated that the strategy singular specialists answer assaults from outside the association may bring about information taking or misfortune. A technique culprits assault is through the system for mental element hacking, by focusing on human discernments and comparing practices (Enrici et al., 2010).

Anderson (2008) considers the 2 fundamental assortments of mental element hacking are pretexting – the usage of outcomes to urge people to supply information after they wouldn't ordinarily – and phishing. Phishing assaults use messages, artificial sites, or malevolent bundle to direct clients to deceptive sites that take individual information, certifications, and fiscal data.

Dohan (2004) expressed that every assortment of assaults either get the opportunity to determine social connections to accumulate trust and duty or to control observation, conviction, and conduct to impel feelings of delight or concern. On the off chance that some person succumbs to mental element hacking, pariahs could take, harm, or pulverize organization or individual information. Serving to individuals see the potential existing dangers and dangers concerned could encourage enterprises and individuals enough safeguard their information.

CHAPTER 3
THEORETICAL FRAMEWORK

3.1Internet Security

10 years past, the net was one thing singularly "techies" talked with respect to. It completely was a substitution boundless supply of information, with just a couple of clients. Today, the net has as of now turned into an essential a piece of our lives. It's wherever we tend to get to our managing an account records, MasterCard proclamations, expense forms and distinctive delicate individual information. By the highest point of this decade, over a couple of billion people are joined with the Internet-that is in regards to 0.5 the world's present populace. However with all the pleasant things the net offers United States, it also opens the way to genuine, likely destroying dangers. Not care for organization and government tablet frameworks, couple of PCs have any shields on the far side essential infection security (BigPlanet, 2010). Which implies at whatever time you're on-line, you're a conceivable focus for on-line culprits and programmers? Also, in the event that you have fast web get to, your portable PC is on-line more often than not, making web hoodlums and programmers a 24-hour-a-day, year-round danger to you, your own information, and your gang.

When you get to the net, your portable workstation communicates something specific over the net that unambiguously recognizes your tablet and wherever it's set. This empowers the information you've asked for to be come to you. Frequently, this asked for information conveys with it undesirable concealed programming framework made by programmers and on-line lawbreakers. This product framework introduces itself on your portable workstation and may either be essentially an irritation or make a great deal of genuine risk to you, your personality and delicate cash information. Here and there the annoyances are unmistakable and easy to spot, though the great deal of risky dangers are generally undetectable, quiet, and intense to discover till it's past the point of no return (BigPlanet, 2010).

A few cookies are innocuous on-line military operation and interest devices. The heft of adware comprises of pop-up promotions that are simply uninvited disturbances. The matter is that programmers and on-line offenders are dynamically exploitation cookies and adware to discreetly sneak onto your portable workstation and to get to your own information while not your information. This "spyware" watches and records all that you are doing on-line, exertion your passwords, individual record information, and diverse individual and touchy information powerless. Once caught, this information is frequently sent back to on-line crooks to be utilized as a part of getting to your own information, taking your personality, and your money (BigPlant, 2010).

3.1.1 Online privacy

Protection are regularly seen as a limit administration system wherever an individual characterizes with whom he can impart and what kind of correspondence (and however much) can happen (Mekovce and Hutinski, 2012). Limit administration permits the genuine individual to understand the predefined level of contact with others, at a chose time and in accordance with unequivocal conditions. 2 assortments of elements have an impact on the system for limit control: (1) situational variables and (2) individual elements. Situational elements appreciate social and physical segments. Social parts talk over with the presence of others with whom the individual will convey others' attributes, and attitude to speak (Mekovce and Hutinski, 2012). Physical segments talk over with physical boundaries, area and separation. Individual elements are connected with people's attributes, similar to their need for security. On-line protection is subsequently laid out as partner trade of web clients' close to home information for a couple edges (Mekovce and Hutinski, 2012). On the inverse hand, the term on-line protection is once in a while associated with information security and in this manner is portray as web clients' contemplations concerning their capacity to deal with the social occasion of their own information, in like manner on administration the long run use of the gathered information or the information that were created bolstered their on-line exercises (Mekovce and Hutinski, 2012). In accordance with their contemplations concerning information protection individuals are regularly arranged in 3 groups (Mekovce and Hutinski, 2012): (1) security guardians, (2) information dealers and (3) comfort seekers. Securities guardians’ are individuals who are unpleasantly included with respect to their information protection. Information dealers are more individuals who can exchange their own information for a tiny/low honor. Comfort seekers however recognized data variety incorporates on-line gathering activity data gathered by means of intelligent on-line looking or on-line mail index. All through un-volunteered however overlooked data grouping snap streams data on web use are gathered. Data use strategy incorporates the ensuing data operations: offering, data uncovering to third gatherings and data deal to third gatherings (Mekovce and Hutinski, 2012).

3.1.2 Online security

Initial step of security associated administration is that the recognizable proof and characterization of data that require to be ensured. Once it’s incredible what should be ensured, subsequent inquiry is anyway it should be secured (Mekovce and Hutinski, 2012). Information security is frequently laid out as an order that uses the thoughts of privacy, honesty, and accommodation to answer the subject of however data should be ensured (Mekovce and Hutinski, 2012). This CIA triad is upheld exploitation various ensuring components like coding, validation, interruption discovery and so forth inquiries that should be addressed once adapting to the insurance of information security are (Mekovce and Hutinski, 2012). On-line clients are continuously getting themselves presented to security dangers all through their on-line exercises. Security dangers grasp the dangers like control with information and/or systems (e.g. annihilation, mercantilism or adjustment of information) or various assortments of misrepresentation and abuse (Mekovce and Hutinski, 2012). Seen on-line security is sketched out as on-line clients’ impression of anyway they’re ensured against dangers connected with security. Kim et al. (2010) utilized the term Perceived Security Protection (PSP) to clarify buyers’ discernment that the net merchandiser can satisfy security necessities, (for example, validation, honesty, and encryption). Two primary variables with respect to saw security in e-business are frequently recognized (Mekovce and Hutinski, 2012): (1) saw operational issue and (2) saw approach related issue. Seen operational issue incorporates activities that a site will go for ensure that the clients feel secure all through the web collaboration. On one hand, saw operational issue incorporates: the webpage’s impedance of unapproved access; weight on login name and parole verification; subsidizing and spending plan spent on security; perception of client consistence with security methods; joining of dynamic frameworks; conveyance of security things at interims the webpage; site's coding system; and union with system security merchants. On the inverse hand, saw strategy related issue incorporates the resulting things: online webpage's weight on system security; high administration responsibility; push to frame clients tuned into security methodology; the site's staying up with the latest with item measures; the site's weight on security in document exchanges; and issues in regards to the web program (Mekovce and Hutinski, 2012).

3.1.3 Spyware: the new virus

If you're even an off-the-cuff person, likelihood is that you've detected regarding viruses and what they'll do to your laptop. Viruses are serious threats that attack your laptop and information, and customarily disrupt your life; however they aren't wont to steal your sensitive personal data. Web criminals produce spyware to try to steal. They require you to believe that anti-virus software system is all the protection you would like. As necessary because it is to your security, anti-virus software system can't find or stop this newer, a lot of refined threat from coming into your laptop. Stopping spyware needs even larger protection (BigPlanet, 2010).

Spyware represents a replacement, a lot of dangerous threat than viruses. What makes spyware therefore destructive? It attacks laptop. Here's a side-by-side comparison:

Table 3.1: Comparison between virus and spyware **(**BigPlanet, 2010)

Virus	Spyware
Damages data	Steals sensitive private information
Written by hackers	Written by professional online criminals
Infection is obvious and can be detected with anti-virus software	Infection is silent and cannot by detected with anti-virus software
Most computer users are sufficiently protected	Very few computer users are protected
The threat is decreasing	The threat is increasing

3.2 Malware

Malware which is a short form for Malicious software is a generalized word used to refer to different types of intrusive or of unfriendly software like worms, Trojan horses, computer viruses, and other malicious programs which can take the form of scripts, active content, executable code, and other software. Below are some categories of malware popular for computer.

3.2.1Trojan horses

For a malicious program to achieve its objectives, it must have the capacity to keep running without being recognized, closed down, or erased. At the point when a malicious program is camouflaged as something normal or alluring and unknowingly users install them in their computers. This is the system of the Trojan horses or Trojan. In expansive terms, a Trojan horse is any program that welcomes the client to run it, covering destructive or malicious executable code of any portrayal. The code may produce results instantly and can prompt numerous undesirable impacts, for example, encoding the client's documents or downloading and executing further malicious usefulness (Abrams and Podell, 2011).

On account of some spyware, adware, and so on the supplier may require the client to recognize or acknowledge its installation, depicting its conduct in loose terms that may effortlessly be misjudged or overlooked, with the expectation of misdirecting the client into introducing it without the supplier in fact in break of the law (Abrams and Podell, 2011).

3.2.2Computer Viruses

A computer virus program typically covered up inside another apparently harmless program that creates duplicates of itself and inserts them into different or other files or programs, and that ordinarily performs a malicious activity, (for example, data destruction) (Kirat et al., 2014).

3.2.3Rootkits

Once a malicious program is installed on a computer system, it is fundamental that it stays disguised, to maintain a strategic distance from identification. Software programs known as rootkits permit this disguise, by altering the user's computer operating system so that the malware is avoided the client. Rootkits can keep a malicious procedure from being obvious in the computer system's list, or keep its documents from being perused (Kirat et al., 2014).

A few malicious programs contain schedules to guard against evacuation, not only to conceal them. An early illustration of this conduct is recorded in the Jargon File story of a couple of programs invading a Xerox CP-V time sharing framework (Kirat et al., 2014).

3.2.4Computer Worms

A computer worm is a completely independent computer malware program that can duplicate itself so as to spread to different computers. Regularly, it utilizes a computer network to spread itself, depending on security failures on the target computer to get to it. Unlike a computer virus, it does not have to append itself to a current program (Al-Salloum and Wolthusen, 2010).

3.2.5. Keylogging

Keystroke logging, which is preferably known as keylogging, is a situation whereby key struck on keyboard are recorded, basically in an unnoticed way so that the user using the keyboard is unaware that their actions are being monitored. There are various types of keylogging ranging from hardware and software-based approaches to acoustic analysis (Owusu et al., 2012).

3.3 Possible Signs Users Can Use to Know Computer Threats

Possibilities are users might have been a victim of attack via the Internet and they are not even aware of it. The fact is over 90% user of the Internet have one or more spyware hanging around their computers with them being aware of it. Therefore for the users to protect them self from these threats, the user need to know how to identify the common signs that accompanying these threats or attacks. Below are some of the possible signs/symptoms users might be experiencing presently experiencing include (BigPlanet, 2010):

- ***Unwanted emails increment:*** This increment in email is an aftereffect of individual data gathered by cookie programs that is sent back to the originator of cookie, and afterward sold to other web advertising firms.
- ***Pop-up of unwanted online advertisement***: The program that causes pop-ups to show up on user’s computer is a type of spyware, and is stacked on their computer without their insight when they visit certain websites.
- ***Change of browser homepage without your cognition***: Some specific websites will stack cookies into user’s computer and changes their homepage automatically to their webpage. It is a disturbance that happens every now and again to Internet clients.
- ***The user’s computer operate slower than normal***: Spyware stacked user’s computer uses the same computer memory that is expected to run user’s more relevant software programs. This leads to competition for memory in user’s computer, causing the greater part of your more basic software programs to run more slowly than usual.

3.3.1 Possible steps for users to protect their computers from threats

The outlined steps below in line with good and complete anti-virus software will help users in protecting their information in their computers and many other Internet threats (BigPlanet, 2010).

***Step 1*: Users should search for/find out the threats that are already in their computer:** The primary thing users have to do is to figure out regardless of whether they have spyware or other threatening software on your computer. This needs complete and good Internet security tools that fully scan user's personal information and the tools will help identify system monitors, adware, cookies, Trojan horses etc., and will also scan the websites the user recently visited and alert them if any threat content is found on them.

***Step 2:* Threats Removal:** It is important to remove the threats as soon as possible once they are found in the user's computer. It requires that a user make use of strong and good anti-virus software which can fetch out the adware, cookies, Trojan horse etc. and eliminates them.

***Step 3:* User should create a protective wall around their computer:** Once all potential dangerous threats and cookies have been eliminated from user's computer and also continue to stay threat free user should install strong firewall. Firewall supplies a strong barricade between users and possible hackers trying to get access to user's computer.

***Step 4:* Internet junks should be filtered out:** This is done by managing the content and use of computer and this done by installing software that filters web contents. Strong and good software that filter web content lets user decide what program or websites they should give permission to.

CHAPTER 4
METHODOLOGY

4.1 Research Model

This study, which is aimed at investigation of self-efficacy and perception towards computer and Internet security amongst universities students in North part of Iraq, has taken place within the frame of a control group, based on self-efficacy and opinions.

The independent variable of the survey and causal comparative study includes three variables: Gender, Age and Faculty. The dependent variables were Social Networking Sites (SNS), Malicious Software (MS), Web Security & Social Engineering (WSS), and Computer Security (CS).

The 1st, 2nd, 3rd and the 4th research questions of the study have taken place around a scientific framework. Table 4.1 gives the categorization and description of the related items of dependent variables. A figurative view of the research model and the meanings of the used words are given in Figure 4.1.

Table 4.1: Related items of dependent variables of the study

Groups	Items
G_{SNS}	Q1,Q2,Q3,Q4,Q5,Q6,Q7,Q8,Q9,Q10,Q11,Q12
G_{MS}	Q13,Q14,Q15,Q16,Q17,Q18,Q19,Q20,Q21
G_{WSS}	Q22,Q23,Q24,Q25,Q26,Q27,Q28,Q29
G_{CS}	Q30,Q31,Q32,Q33,Q34,Q35

G_{SNS} = Opinions about Social Networking Sites (SNS), G_{MS} = Opinions about Malicious Software (MS), G_{WSS} = Opinions about Web Security & Social Engineering (WSS),G_{CS} = Opinions about Computer Security (CS)

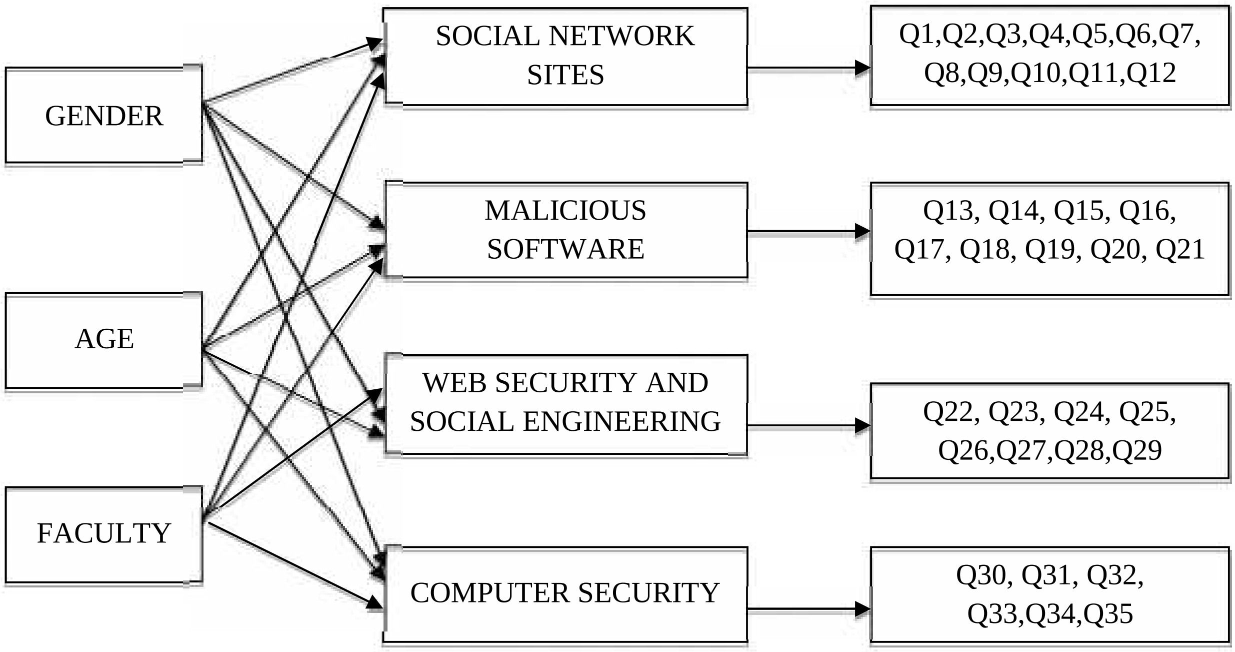
GENDER
AGE
FACULTY
SOCIAL NETWORK SITES
MALICIOUS SOFTWARE
WEB SECURITY AND SOCIAL ENGINEERING
COMPUTER SECURITY
Q1,Q2,Q3,Q4,Q5,Q6,Q7, Q8,Q9,Q10,Q11,Q12
Q13, Q14, Q15, Q16, Q17, Q18, Q19, Q20, Q21
Q22, Q23, Q24, Q25, Q26,Q27,Q28,Q29
Q30, Q31, Q32, Q33,Q34,Q35

Figure 4.1: Research model of the study

4.2 Research Setting

The questionnaire used in this study was developed by Cavus and Ercag (2014). This study has been carried out at these universities (Soran University, Salahaddin University and University of Sulaimani) in both faculties (Faculty of Engineering and Faculty of Arts) in north part of Iraq.

4.3 Participants

The students were chosen randomly and the volunteered participants (students) in this study consisted of total of 709 students, which was made up of 525 undergraduate and 183 postgraduate (Master and PhD) students attending three different universities in North part of Iraq, which are; Soran University, Salahaddin University and University of Sulaimani in (North Iraq) from different class levels and departments in the faculty of arts and engineering. High percentages of the students were from University of Sulaimani and Salahaddin University, with value of 40% and 38% respectively and Soran University was the lowest with 22% of only undergraduate students. 369 students from Faculty of

Engineering and 340 from Faculty of Arts, students were selected without any prior interest group of students in mind. The study was conducted during the 2014-2015 Spring term.

There are 56.84% male and 43.16% female students who joined the study from both Faculties. The characteristics of the respondents are presented in Table 4.2. From the table, there were 32% students that were 18-20 years old of age, 35% students that were 21-23 years old of age, 17.1% students that were 24-26 years old and 15.9% students that were 27+ years old (Table 4.2).

Table 4.2: Important demographic data of participants (N = 709)

Characteristic	Frequency	%
Gender		
Male	403	56.84
Female	306	43.16
Age		
18-20	227	32
21-23	248	35
24-26	121	17.1
27+	113	15.9
Degree		
Undergraduate	525	74
Postgraduate (Ms and PhD)	184	26
Faculty		
Engineering Faculty	369	52
Arts Faculty	340	48

4.4 Instrument

The questionnaire is made up of 4 dimensions SNS, MS, WSS and CS which had 35 items altogether in total. In SNS, 12 items were assigned to it, in order to address the various security problems that arise or may arise from the use of social networking sites. In MS, 9 items were assigned to it, in order to address the various malicious software issues that may arise from using the Internet or computer by students. In WSS, 8 items were assigned to address the various web security and social engineering issues that may arise from the use of the Internet for emails, online shopping etc. by the students. And finally, in CS 6 items were assigned to address the various computer security issues that may possible arise from the use of the computer by the students. The participants answered to items on 5 Likert Scale from "Very Confident" (5 point), "Confident" (4 point), "Neutral" (3 point), "Not Confident" (2 point), and "Not Very Confident" (1 point). Selected items were revised based upon their comments and recommendations. The questionnaire reliability was calculated as 0.95 by using Cronbach's Alpha for 35 items were calculated to be 0.95. According to the results of the reliability result in Table 4.3, it can be seen that the Cronbach's Alpha for each dimensions in the scale were listed from 0.907 CS to 0.840 SNS. Based on this result it was decided that the scale can be used since reliability measurements gave good acceptable results. The result from this study show that the total items (scales) and coefficient of reliability of all groups are above 0.70, hence our findings shows that the scales are reliable (Sipahi, Yurtkoru & Cinko, 2010).

Table 4.3: Reliability test for subscales of the questionnaire

Dimensions	Cronbach's Alpha Reliability
SNS	0.84
MS	0.87
WSS	0.90
CS	0.90

4.5Internet Usage by Students

4.5.1 Hours students spent on the Internet daily

From the result, it was observed as shown Figure 4.2 below, that only 3% spend about 0-1 hour daily, 24.1% spend 2-3 hours daily, 37.9% spend about 4-5 hours daily and 35% spend 6+ hours daily from a population pull of 709 students whom participated in the survey.

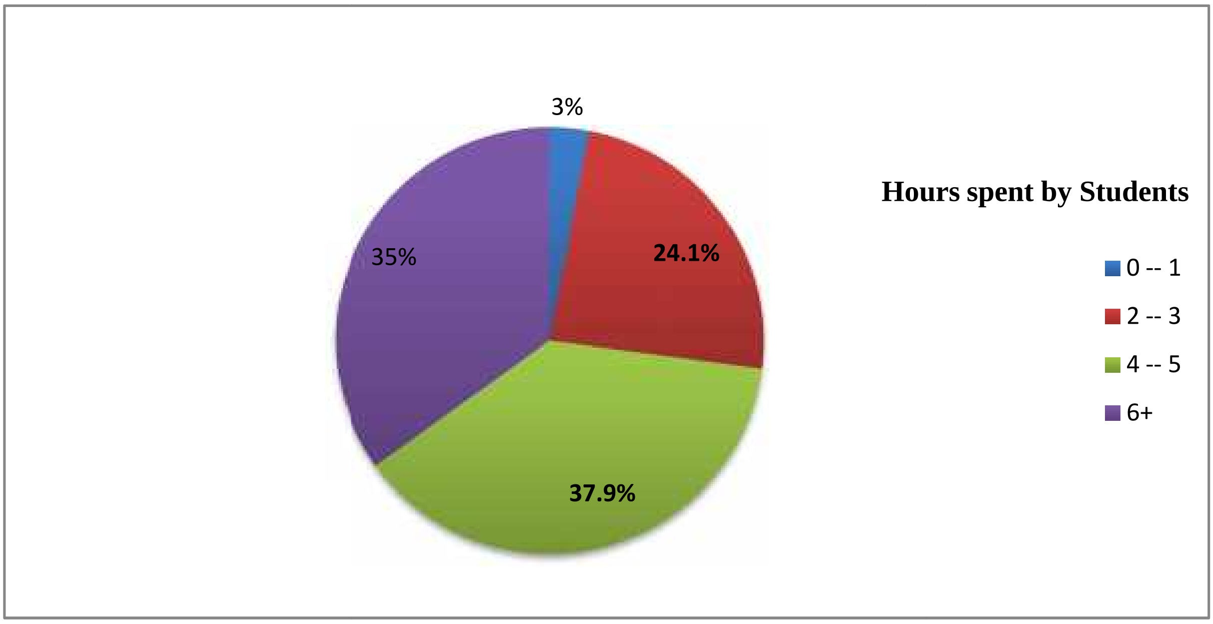

Figure 4.2: Hours students spent using the Internet

4.5.2 Reasons why students use the Internet

From the result reported, it was observed as shown Figure 4.3 below, that only 4.2% use the Internet for online banking reasons, 21.1% use the Internet for e-learning purposes, 2.8% use the Internet for e-commerce purposes, 1.6% use the Internet for e-government purposes, 3.4% use the Internet for online shopping, 24.6% use the Internet for e-mails purposes and 42.3% use the Internet for social media purposes from a population pull of 709 students whom participated in the survey.

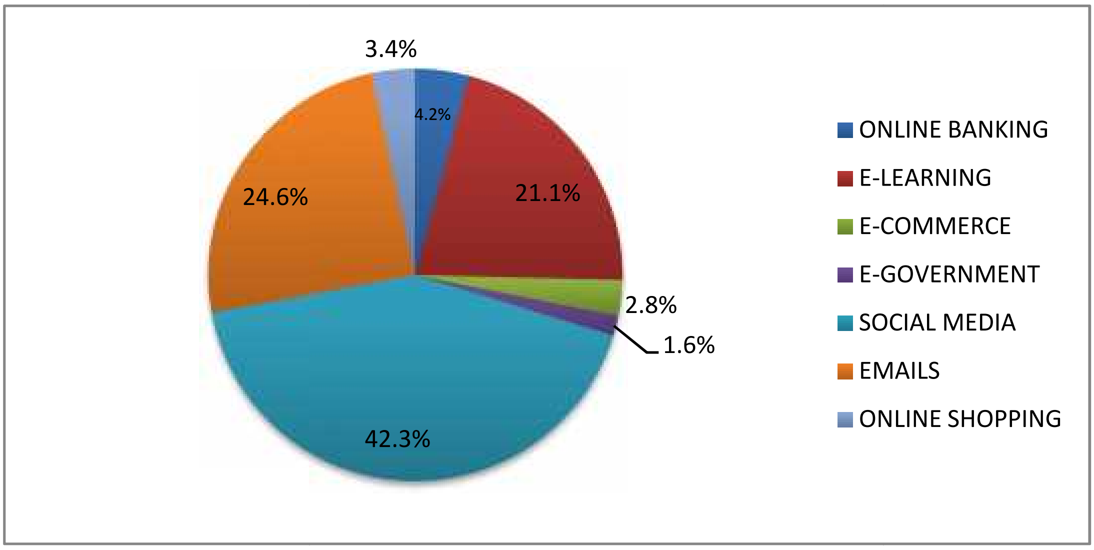

Figure 4.3: Reasons why students use the Internet

4.5.3 Antivirus program usage by students

From the result, it was observed as shown Figure 4.4 below, that only 15% of students do not have antivirus on their computers and about 85% of students do have antivirus on their computers from a population pull of 709 students whom participated in the survey. This result shows that a lot of students make use of antivirus.

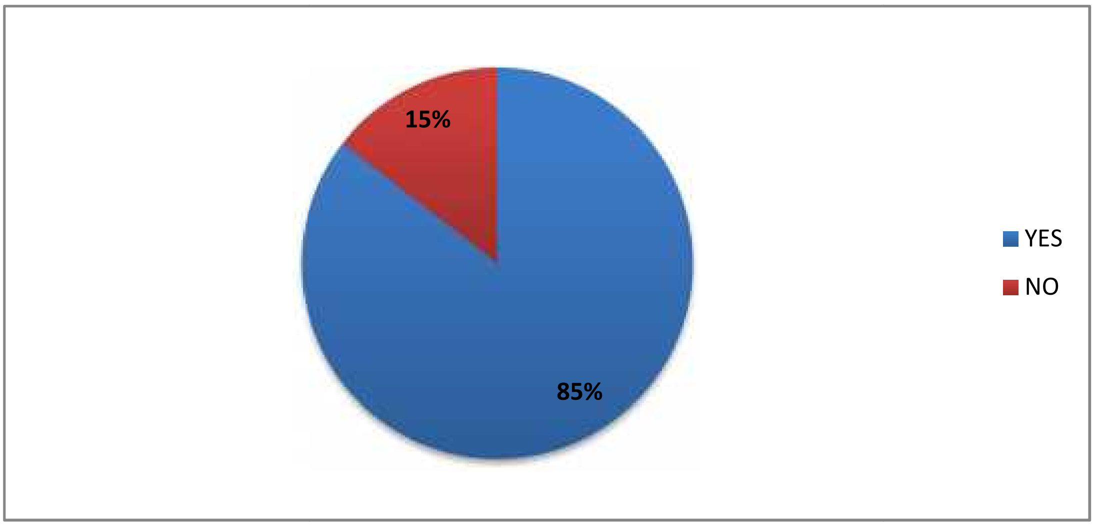

Figure 4.4: Anti-virus program usage by students

4.6 Analysis of Data

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

4.7 Procedure

This study was designed in order to fill the gap in the students' perception towards the use of computer and Internet security in North Iraq. And for this study to be successfully carried questionnaires were given to over 1000 students in various universities in the country for over 1 month. Survey questionnaires were given to students in these universities (Soran University, Salahaddin University and University of Sulaimani) and collected back from randomly volunteered students every 3 days in a week for over 3 weeks. The questionnaires were given to students in different locations, such as the class room, the faculty building, the cafeteria, etc. This study was conducted at Soran University, Salahaddin University and University of Sulaimani in the Faculty of Arts and Engineering in the North part of Iraq during the 2014-2015 Spring semesters. The participants were from undergraduate and postgraduate education levels from different year.

The work was done in a period of over 5 months with a population sample of 709 students, the study was quantitative in nature, and survey with questionnaire was design. The survey was administered to students in three Universities in North part of Iraq. After the collection of questionnaires from the students, a total of only 709 correctly filled questionnaires were recovered from the students from various universities altogether, the accumulated data were subjected to various analysis (such as; frequency and percentage, independent *t*-test and one-way ANOVA) in order to give answer to the aim of the study/research questions of the study. Afterwards the results from the data analysis were discussed in details and conclusion and recommendation were drawn from the results of the study.

CHAPTER 5
RESULTS AND DISSCUSSION

5.1 Student Self-Efficacy and their Perceptions towards Computer and Internet Security

In order to understand the opinions of the students' self-efficacy and their perceptions in the use of computer and Internet security descriptive analysis was employed. From the result shown in Table 5.1, the mean range for all items is "To be able to use Microsoft Security Essentials" (M = 2.9013; SD = 1.20679) which the least mean value out all items which is probably because of the low responses from the web security and social engineering section response they gave and "To be able to add a password to my operating Windows system" (M = 4.0127; SD = 1.18422) which gave the highest mean value out of all items. The total mean and standard deviation values for all 35 items is (M = 3.3173; SD = 0.36169)

Table 5.1: Total mean and standard deviation of the question

Items	Mean	SD
1. To be able to hide the information that I share on social networking sites from people.	3.23	1.48
2. To be able to block requests from people I don't know/want on social networking sites.	3.82	1.29
3. To be able to hide my profile information from people I don't want on social networking sites.	3.52	1.43
4. To be able to protect personal information I share with people on social networking sites.	3.93	1.19
5. To be able to contact the necessary people if my password is taken by someone on social networking sites	3.08	1.47
6. To be able to share videos and photos on social networking sites that will not harm my reputation.	3.05	1.46
7. To be able to share information about others on social networking sites that will not harm their reputation.	3.08	1.47
8. To be able to use social networking sites like Facebook and Twitter in a safe way.	3.07	1.47

Table 5.1: Continued …

9. To be able to protect myself from infected videos on social networking sites.	3.07	1.44
10. To be able to take necessary safety precautions against security breaches on social networking sites.	3.04	1.46
11. To be able to prevent theft of personal photo albums on social networking sites.	3.02	1.48
12. To be able to create a secure password on social networking sites.	3.07	1.47
13. To be able to prevent harmful software from infecting your computer.	3.17	1.43
14. To be able to protect my password from key loggers.	3.26	1.19
15. To be able to clean my computer when it has been infected with viruses.	2.91	1.21
16. To be able to prevent viruses from entering my computer.	3.19	1.41
17. To be able to take the necessary precautions to prevent Trojan horses from entering my computer.	3.25	1.19
18. To be able to protect my computer from worms.	2.90	1.20
19. To be able to protect myself from spyware software.	3.17	1.43
20. To be able to create a very secure password.	3.25	1.19
21. To be able to use Microsoft Security Essentials.	2.90	1.21
22. To be able to do shopping in a secure way via Internet.	3.32	1.45
23. To be able to take the necessary security precautions against spam e-mails.	3.39	1.21
24. To be able to protect myself from built-in camera pens and glasses from social engineering attacks.	3.03	1.27
25. To be able to protect myself from social engineering attacks via e-mails.	3.03	1.27
26. To be able to use the necessary precautions while using interactive banking on the Internet.	3.29	1.43
27. To be able to use the necessary precautions against hoax e-mails.	3.40	1.20
28. To be able to protect myself from phishing e-mails.	3.04	1.27
29. To be able to show the difference between HTTP and HTTPS.	3.03	1.27
30. To be able to protect my personal files.	3.85	1.17
31. To be able to take the necessary security measures for logging on to my computer.	3.92	1.19
32. To be able to add a password to my operating Windows system.	4.01	1.18
33. To be able to update my security files.	3.95	1.19
34. To be able to add a password to my files.	3.95	1.23
35. To be able to create backup files in case of problems.	3.92	1.21
Total	**3.32**	**0.36**

5.1.1 Social networking sites

In order to understand the students' self-efficacy and perceptions of the use of computer and Internet security based on Social Networking Sites, descriptive analysis was employed. According to the result on Social Networking Sites, the students gave very clear opinions based on their perspectives on what they practices in terms of computer and Internet security over social networking sites. From the result shown in Table 5.2, the mean range for all items is "To be able to prevent theft of personal photo albums on social networking sites" (M = 3.0197; SD = 1.47662) which the least mean value out all items and "To be able to protect personal information I share with people on social networking sites" (M = 3.9337; SD = 1.18720) which gave the highest mean value out of all items. The total mean and standard deviation values for all 12 items is (M = 3.2478; SD = 0.32614).

Table 5.2: Mean and standard deviationfor each item of SNS

Social Networking Sites (SNS)	**Mean**	**SD**
1. To be able to hide the information that I share on social networking sites from people.	3.23	1.48
2. To be able to block requests from people I don't know/want on social networking sites.	3.82	1.29
3. To be able to hide my profile information from people I don't want on social networking sites.	3.52	1.43
4. To be able to protect personal information I share with people on social networking sites.	3.93	1.19
5. To be able to contact the necessary people if my password is taken by someone on social networking sites	3.08	1.47
6. To be able to share videos and photos on social networking sites that will not harm my reputation.	3.05	1.46
7. To be able to share information about others on social networking sites that will not harm their reputation.	3.08	1.47
8. To be able to use social networking sites like Facebook and Twitter in a safe way.	3.07	1.47
9. To be able to protect myself from infected videos on social networking sites.	3.07	1.44
10. To be able to take necessary safety precautions against security breaches on social networking sites.	3.04	1.46
11. To be able to prevent theft of personal photo albums on social networking sites.	3.02	1.48
12. To be able to create a secure password on social networking sites.	3.07	1.47
Total	**3.25**	**0.33**

5.1.2 Malicious software

In order to understand the students' self-efficacy and perceptions of the use of computer and Internet security based on Malicious Software, descriptive analysis was employed. According to the result on Malicious Software, the students gave very clear opinions based on their perspectives on what they practices in terms of computer Internet security over Malicious Software. From the result shown in Table 5.3, the mean range for all items is "To be able to use Microsoft Security Essentials" (M = 2.9013; SD = 1.20679) which the least mean value out all items and "To be able to create a very secure password" (M = 3.2581; SD = 1.18713) which gave the highest mean value out of all items. The total mean and standard deviation values for all 9 items is (M = 3.1108; SD = 0.16006).

Table 5.3: Mean and standard deviationfor each item of MS

Malicious Software (MS)	**Mean**	**SD**
1. To be able to prevent harmful software from infecting your computer.	3.17	1.43
2. To be able to protect my password from key loggers.	3.25	1.19
3. To be able to clean my computer when it has been infected with viruses.	2.91	1.21
4. To be able to prevent viruses from entering my computer.	3.19	1.41
5. To be able to take the necessary precautions to prevent Trojan horses from entering my computer.	3.25	1.19
6. To be able to protect my computer from worms.	2.90	1.20
7. To be able to protect myself from spyware software.	3.17	1.43
8. To be able to create a very secure password.	3.26	1.19
9. To be able to use Microsoft Security Essentials.	2.90	1.21
Total	**3.11**	**0.16**

5.1.3 Web security and social engineering

In order to understand the students' self-efficacy and perceptions of the use of computer and Internet security based on Web Security and Social Engineering, descriptive analysis was employed. According to the result on Web Security & Social Engineering, the students gave very clear opinions based on their perspectives on what they practices in terms of computer and Internet security over Web Security & Social Engineering. From the result shown in Table 5.4, the mean range for all items is "To be able to protect myself from social engineering attacks via e-mails" (M = 3.0268; SD = 1.26697) which the least mean value out all items and "To be able to take the necessary security precautions against spam e-mails" (M = 3.3977; SD = 1.20895) which gave the highest mean value out of all items. The total mean and standard deviation values for all 8 items is (M = 3.1917; SD = 0.17414).

Table 5.4: Mean and standard deviationfor each item of WSS

Web Security & Social Engineering (WSS)	**Mean**	**SD**
22. To be able to do shopping in a secure way via Internet.	3.32	1.45
23. To be able to take the necessary security precautions against spam e-mails.	3.40	1.21
24. To be able to protect myself from built-in camera pens and glasses from social engineering attacks.	3.03	1.27
25. To be able to protect myself from social engineering attacks via e-mails.	3.03	1.27
26. To be able to use the necessary precautions while using interactive banking on the Internet.	3.29	1.43
27. To be able to use the necessary precautions against hoax e-mails.	3.39	1.20
28. To be able to protect myself from phishing e-mails.	3.04	1.27
29. To be able to show the difference between HTTP and HTTPS.	3.03	1.27
Total	**3.19**	**0.17**

5.1.4 Computer security

In order to understand the students' self-efficacy and perceptions of the use of computer and Internet security based on Computer Security, descriptive analysis was employed. Also according to the result on Computer Security, the students gave very clear opinions based on their perspectives on what they practices in terms of computer and Internet security over Computer Security. From the result shown in Table 5.5, the mean range for all items is "To be able to protect my personal files" (M = 3.8505; SD = 1.17420) which the least mean value out all items and "To be able to add a password to my operating Windows system" (M = 4.0127; SD = 1.18422) which gave the highest mean value out of all items. The total mean and standard deviation values for all 6 items is (M = 3.9335; SD = 0.05340).

Table 5.5: Mean and standard deviationfor each item of CS

Computer Security (CS)	**Mean**	**SD**
30. To be able to protect my personal files.	3.85	1.17
31. To be able to take the necessary security measures for logging on to my computer.	3.92	1.19
32. To be able to add a password to my operating Windows system.	4.01	1.18
33. To be able to update my security files.	3.95	1.19
34. To be able to add a password to my files.	3.95	1.23
35. To be able to create backup files in case of problems.	3.92	1.21
Total	**3.93**	**0.05**

5.2Student Self-Efficacy and their Perceptions towards Computer and Internet Security Based on Gender Differences

In order to understand the students' self-efficacy and perceptions of Internet and computer use between both genders independent samples *t*-test was employed. According to the Table 5.6, concerning the self-efficacy and user's perception towards computer and Internet security, there are statistically significant differences between genders in this study (p<.05).

Table 5.6: Difference between genders

	Gender	**N**	**Mean**	**SD**	**Mean Difference**	**t**	**p**
SNS	Male	403	3.65	1.03	.175	2.038	**.042***
	Female	306	3.48	1.16			
MS	Male	403	3.48	1.13	.464	4.720	**.000***
	Female	306	3.01	1.23			
WSS	Male	403	3.53	1.11	.454	4.650	**.000***
	Female	306	3.07	1.19			
CS	Male	403	3.23	1.26	.079	.787	.431
	Female	306	3.15	1.35			

Where; Computer Security (CS); Web Security & Social Engineering (WSS); Malicious Software (MS); Security on Social Networking Sites (SNS): Total sampled population (N); Standard Deviation (SD) and * means p<0.05 (there exist statistical significant difference)

From the independent *t*-test result as shown in Table 5.6, there existed significant difference ($p<0.05$) between SNS, MS, and WSS in both male and female. But on the other hand, looking at the results of Computer security, there is no statistically significant difference between gender ($p>0.05$). Male students had higher means values in SNS, MS, WSS than female students but in CS the means differences was very close. However, from the research results, it could be cited that male and female students have different security perception towards computer and Internet security. The close mean difference in the choice of Computer security between males and females, maybe due to the fact that both sexes pay more attention or are more carefully when it comes to their personal computer well-being and their files, most important since they are students.

However, Suri and Sharma (2013), results showed that no significant difference ($p>0.05$) exists between gender and attitude towards computer and e-learning. But Genis-gruber and Gonul (2012) reported that significant differences ($p<0.05$) existed on gender in both technology acceptance and user behavior. The variation between the genders lies in perceptions of technology, where subjective norms and ease of use influence female's perceptions (Genis-gruber and Gonul, 2012). And they stated that there exist statistically significant difference between gender towards online shopping (Genis-gruber and Gonul, 2012).

Different studies on the impact of gender on the behavior of students prior to e-learning have been carried out (Egbo et al., 2011, Abedalaziz et al., 2013, Laiw and Huang, 2011, Suri et al., 2014). Egbo et al (2011) cited from their study that female students accept computer use than male students. On the contrary, Liaw and Huang (2011) showed that male students have better e-learning behavior than female students. Bebetsosi and Antoniou (2009) showed that gender difference existed in-relation to computer usage. Suri et al. (2014) indicated that there is also gender difference existed in-relation to computer usage.

5.3Student Self-Efficacy and their Perceptions towards Computer and Internet Security Based on Age Differences

In order to understand the students' self-efficacy and perceptions of computer and Internet use between different ages, one-way ANOVA was employed. As indicated in Table 5.7, in this study there are statistically significant differences between in all ages towards computer and Internet security (p<0.05).

Table 5.7: Differences between Ages

Groups	Age	N	Mean	SD	Mean Square	F	p
SNS	18-20	227	3.664	.931	3.401	3.642	**.013***
	21-23	248	3.701	1.060			
	24-26	121	3.525	1.034			
	27+	113	4.000	.930			
	Total	709	3.687	.972			
MS	18-20	227	3.673	.873	11.997	14.668	**.000***
	21-23	248	3.462	.958			
	24-26	121	3.606	.998			
	27+	113	4.320	.872			
	Total	709	3.701	.930			
WSS	18-20	227	3.627	.835	4.636	5.946	**.001***
	21-23	248	3.443	.916			
	24-26	121	3.626	1.006			
	27+	113	3.920	.893			
	Total	709	3.629	.892			
CS	18-20	227	3.594	.885	2.475	2.753	**.042***
	21-23	248	3.528	1.035			
	24-26	121	3.455	1.023			
	27+	113	3.853	1.062			
	Total	709	3.592	.952			

Where; Computer Security (CS); Web Security & Social Engineering (WSS); Malicious Software (MS); Security on Social Networking Sites (SNS): Total sampled population (N); Standard Deviation (SD) and * means p<0.05 (there exist statistical significant difference)

In all groups age category 27+ had the highest mean values and it is significantly difference from every other age groups in all question category. This result suggests that students in different ages pay more attention to computer and Internet security. Stephen et al. (2003) showed that there is age based difference in-relation to computer usage from the survey they did on various individual of different age groups.

Table 5.8 shows the multiple comparisons of all age groups. This compares the age group in each section within each group between the ages. In SNS, MS, WSS and CS, there is significant difference in age group 27+ but in other age group (i.e., 18-20, 21-23, 24-26) there are no significance differences (Table 5.8). From Table 5.8., there is statistical difference between age group 18-20 with 27+ but there is no significant difference between age group 18-20 with 21-23 and 24-26, age group 21-23 showed no significant difference between all age groups, age group 24-26 showed no statistical significant difference between age 18-20 and 21-23 but there is significant difference between age group 27+ and age group 27+ showed significant difference between age group 18-19 and 24-26 but there is no significant difference between age 21-23 in SNS.

In MS, there is statistical difference between age group 18-20 with 27+ but there is no significant difference between age group 18-20 with 21-23 and 24-26, age group 21-23 showed significant difference with 27+ but there is no significant difference between age group 18-20 with 21-23 and 24-26, age group 24-26 showed significant difference with 27+ but there is no significant difference between age group 18-20 with 21-23 and 27+ showed significant difference between all age groups.

In WSS, there is statistical difference between age group 18-20 with 27+ but there is no significant difference between age group 18-20 with 21-23 and 24-26, age group 21-23 showed significant difference with 27+ but there is no significant difference between age group 18-20 with 21-23 and 24-26, age group 24-26 showed no significant difference between all age groups, and age group 27+ showed significant difference between age group 18-19 and 21-23 but there is no significant difference between age 24-26.

In CSS, there are no significance differences between all age groups in all age categories.

Table 5.8: Multiple comparisons of age based difference

Dependent Variable	(I) AGE	(J) AGE	Mean Difference (I-J)	Std. Error	95% Confidence Interval	
					Lower Bound	Upper Bound
SNS	18-20	21-23	-.04321	.11234	-.3359	.2495
		24-26	.13908	.11320	-.1562	.4343
		27+	**-.33566***	.11643	-.6408	-.0305
	21-23	18-20	.04321	.11234	-.2495	.3359
		24-26	.18229	.14624	-.1997	.5643
		27+	-.29245	.14875	-.6822	.0973
	24-26	18-20	-.13908	.11320	-.4343	.1562
		21-23	-.18229	.14624	-.5643	.1997
		27+	**-.47475***	.14940	-.8664	-.0831
	27+	18-20	**.33566***	.11643	.0305	.6408
		21-23	.29245	.14875	-.0973	.6822
		24-26	**.47475***	.14940	.0831	.8664
MS	18-20	21-23	.21140	.10215	-.0547	.4775
		24-26	.06760	.10882	-.2162	.3514
		27+	**-.64634***	.10920	-.9326	-.3601
	21-23	18-20	-.21140	.10215	-.4775	.0547
		24-26	-.14380	.13682	-.5012	.2136
		27+	**-.85774***	.13713	-1.2170	-.4984
	24-26	18-20	-.06760	.10882	-.3514	.2162
		21-23	.14380	.13682	-.2136	.5012
		27+	**-.71394***	.14217	-1.0866	-.3413
	27+	18-20	**.64634***	.10920	.3601	.9326
		21-23	**.85774***	.13713	.4984	1.2170
		24-26	**.71394***	.14217	.3413	1.0866

Table 5.8: Continued …

WSS	18-20	21-23	.18364	.09770	-.0709	.4382
		24-26	.00078	.10884	-.2832	.2847
		27+	**-.37296***	.11470	-.6737	-.0722
	21-23	18-20	-.18364	.09770	-.4382	.0709
		24-26	-.18287	.13470	-.5347	.1690
		27+	**-.55660***	.13947	-.9222	-.1910
	24-26	18-20	-.00078	.10884	-.2847	.2832
		21-23	.18287	.13470	-.1690	.5347
		27+	-.37374	.14749	-.7604	.0129
	27+	18-20	**.37296***	.11470	.0722	.6737
		21-23	**.55660***	.13947	.1910	.9222
		24-26	.37374	.14749	-.0129	.7604
CS	18-20	21-23	.06610	.10921	-.2185	.3507
		24-26	.13986	.11134	-.1506	.4303
		27+	-.25893	.12981	-.5994	.0816
	21-23	18-20	-.06610	.10921	-.3507	.2185
		24-26	.07376	.14377	-.3018	.4493
		27+	-.32503	.15851	-.7405	.0905
	24-26	18-20	-.13986	.11134	-.4303	.1506
		21-23	-.07376	.14377	-.4493	.3018
		27+	-.39879	.15998	-.8183	.0207
	27+	18-20	.25893	.12981	-.0816	.5994
		21-23	.32503	.15851	-.0905	.7405
		24-26	.39879	.15998	-.0207	.8183

* The mean difference is significant at the 0.05 level.

5.4Student Self-Efficacy and their Perceptions towards Computer and Internet Security Based on Faculty Differences

In order to understand the students' self-efficacy and perceptions of computer and Internet use among students from different faculties, independent samples *t*-test was employed. As indicated in Table 5.9, in this study there are statistically significant differences between both faculty towards computer and Internet security (p<0.05).

Table 5.9: Differences between faculties

	Faculty	N	Mean	SD	Mean Difference	t	p
SNS	Engineering	369	3.72	.99	.654	8.421	**.000***
	Arts	340	3.07	.95			
MS	Engineering	369	3.56	1.11	.612	6.450	**.000***
	Arts	340	2.94	1.16			
WSS	Engineering	369	3.66	1.04	.730	8.173	**.000***
	Arts	340	2.93	1.04			
CS	Engineering	369	3.46	1.16	.596	6.362	**.000***
	Arts	340	2.87	1.26			

Where; Computer Security (CS); Web Security & Social Engineering (WSS); Malicious Software (MS); Security on Social Networking Sites (SNS): Total sampled population (N); Standard Deviation (SD) and * means p<0.05 (there exist statistical significant difference)

From the independent *t*-test result as shown in Table 5.9, there existed significant difference (p<0.05) between SNS, MS, WSS and CS in both Faculties. Faculty of engineering students had higher means values in SNS, MS, WSS and CS than faculty of Art. This result suggests that students in Engineering faculties pay more attention to computer and Internet security than students in Art faculties. This might due the faculty computer applications by engineering students than that of Arts students. Looking at the values in Table 5.9, it is clear that while students from the Engineering faculties pay more attention to computer and Internet security, students from the faculty of Arts pay less attention to computer and Internet security. From the result reported in Table 5.9, it was observed that there is Faculty difference based on Security on Social Networking Sites, Malicious software, Web security and social engineering and computer security based on the statistical significant difference ($p<0.05$) observed among the both faculties. Faculty of engineering students had the highest mean, which might suggest that they have more of computer due to study major, compared to faculty of Arts students.

Odell et al. (2010) indicated that students from faculty of science make use of the Internet most than students from faculty of social science. In the same line Anderson (2010) reported that there is faculty based difference regards computer usage from a survey done on various students from different departments. Also Sam et al. (2011) study on undergraduate students from University Malaysia Sarawak showed that students from faculty of science used the Internet more than students from faculty of arts. This shows that students in faculty of engineering and science make use of their computer than other faculty.

5.5 Age, Gender, Faculty Based Differences With Respect to Total Average of Whole Questionnaire

5.5.1 Age based difference on total average score

Total average score was calculated by adding the responses of students and dividing this into total number of items in the questionnaire.

In order to understand the students' self-efficacy and perceptions of computer and Internet use between different ages, on total average score, one-way ANOVA was employed. As indicated in Table 5.10 and 5.11, in this study there are statistically significant differences between in all ages towards computer and Internet security ($p<0.05$). In all groups age category 27+ had the highest total mean values and it is significantly difference from every other age group in all question categories.

Table 5.10: Age based difference on total average score

Age Groups	N	Mean	SD	Mean square	F	p
18-20	227	3.252	.867	8.707	11.757	**.000***
21-23	248	3.454	.823			
24-26	121	3.201	.837			
27+	113	3.84	.904			
Total	709	3.342	.880			

* The mean difference is significant at the 0.05 level.

Table 5.11, there is statistical difference between age group 18-20 with 27+ but there is no significant difference between age group 18-20 with 21-23 and 24-26, age group 21-23 with 27+ but there is no significant difference between age group 18-20 and 24-26, age group 24-26 showed no statistical significant difference between age 18-20 and 21-23 but there is significant difference between age group 27+ and age group 27+ showed significant difference between all age groups.

Table 5.11: Multiple comparisons of age based difference on total average score

(I) AGE	(J) AGE	Mean Difference (I-J)	Std. Error	95% Confidence Interval	
				Lower Bound	Upper Bound
18-20	21-23	-.23302	.09031	-.4682	.0021
	24-26	.05044	.09396	-.1945	.2954
	27+	**-.58698***	.11243	-.8817	-.2922
21-23	18-20	.23302	.09031	-.0021	.4682
	24-26	.28346	.11610	-.0198	.5867
	27+	**-.35395***	.13150	-.6987	-.0092
24-26	18-20	-.05044	.09396	-.2954	.1945
	21-23	-.28346	.11610	-.5867	.0198
	27+	**-.63741***	.13403	-.9889	-.2859
27+	18-20	**.58698***	.11243	.2922	.8817
	21-23	**.35395***	.13150	.0092	.6987
	24-26	**.63741***	.13403	.2859	.9889

* The mean difference is significant at the 0.05 level.

5.5.2 Gender based difference on total average score

In order to understand the students' self-efficacy and perceptions of computer and Internet use between different genders on total average score, independent samples *t*-test was employed. According to the Table 5.12, concerning the total average perception of the students on the 35 items in all section, there are statistically significant differences between the total means score of both male and female students in this study (p< 05). Male students had higher total means values than female students.

Table 5.12: Gender based difference on total average score

Gender	N	Mean	SD	Mean Difference	t	p
Male	403	3.439	.922	.256	3.372	**.001***
Female	306	3.183	.856			

* The mean difference is significant at the 0.05 level.

5.5.3 Faculty based difference on total average score

In order to understand the students' self-efficacy and perceptions of computer and Internet usebetween different faculties on total average score, independent samples *t*-test was employed. As indicated in Table 5.13, in this study there are statistically significant differences between the total means score of both faculty towards computer and Internet security (p<0.05). Faculty of Engineering students had higher total means values than faculty of Art.

Table 5.13: Faculty based difference on total average score

Faculty	N	Mean	SD	Mean Difference	t	p
Engineering	369	3.550	.674	.540	9.061	**.000***
Arts	340	3.011	.903			

* The mean difference is significant at the 0.05 level.

According to the Table 5.14, in SNS, although students from both faculties gave positive opinions toward Security on Social Networking Sites (SNS), it is interesting to note that they considered different technical characteristics. Students from faculty of engineering considered the most the characteristic “To be able to hide the information that I share on social networking sites from people” (M=3.97, SD=0.99), “To be able to hide my profile information from people I don’t want on social networking sites” (M=4.09, SD=1.28), “To be able to protect personal information I share with people on social networking sites” (M=3.61, SD=1.27) and “To be able to protect myself from infected videos on social networking sites” (M=4.01, SD=1.02). In a similar fashion, from the survey questionnaire, there were technical characteristics and differences that engineering students did not consider much. The least considered characteristic that students from engineering faculty did not consider were “To be able to contact the necessary people if my password is taken by someone on social networking sites” (M=3.47, SD=1.23) but was much considered by faculty of Arts students (M=3.87, SD=1.32) and “To be able to share videos and photos on social networking sites that will not harm my reputation” (M=3.47, SD=1.24) but was much considered by faculty of Arts students (M=3.89, SD=1.32). The least considered characteristic that a student from the engineering faculty is not considered was “To be able to prevent theft of personal photo albums on social networking sites” (M=3.45, SD=1.25). Finally, students from the Art faculty is not considered the characteristic “To be able to hide the information that I share on social networking sites from people” (M=2.48, SD=1.25) and “To be able to protect personal information I share with people on social networking sites” when choosing the given opinions on computer and Internet security on social networks sites. It was assumes that the reason of this difference is probably because faculties have structural differences between themselves even though they are all social network sites users. Salleh et al. (2011) cited that Social Networking Sites (SNS) such as MySpace, Twitter, Facebook, etc., has become a regular occurrence that change that way communication and interaction exist between people. According to Carruth and Ginsburg (2014) indicated that SNS in now ubiquitous in our society and culture, mostly because of Internet usage.

According to the Table 5.14, in MS, although students from both faculties gave good opinions toward Malicious Software (MS), it is interesting to note that they considered different technical characteristics. Students from faculty of engineering considered the most the characteristic “To be able to prevent harmful software from infecting your computer” (M=4.58, SD=0.79), “To be able to clean my computer when it has been infected with viruses” (M=3.80, SD=1.17), and “To be able to take the necessary precautions to prevent Trojan horses from entering my computer” (M=4.13, SD=1.05). This might be because “To be able to use Microsoft Security Essentials” (M=3.78, SD=1.15)”. In a similar fashion, from the survey questionnaire, there were technical characteristics and differences that engineering students did not consider much. The least considered characteristic that students from both faculties did not consider much was “To be able to protect my password from key loggers” (M=3.47, SD=1.29; M=3.28, SD=1.33, respectively). This may due to the fact faculty of engineering students were not that very confident about creation of a very secure password “To be able to create a very secure password” (M=3.80, SD=1.17) and faculty of Arts students were least confident, they were mostly between the range of NEUTRAL as shown in the table. It was assumes that the reason of this difference is probably because faculties have structural differences between themselves even though they are all computer users.

According to Liang and Xue (2010) the generality of Internet and computer utilization and the thin line between home and work, damages can be caused not only to organization but also to individuals due to Internet security breaches. Also user can become victim to identify hacker if their information is lost. In-relation to that unsafe and uncontrollable attitude towards the use of Internet can lead to loop holes in the user’s Internet and information security. Bagachi and Udo (2003) stated that Trojan can be used to steal user’s login details of his or her company. D’Arcy et al. (2009) reported that in 2009 CSI survey shows 64.3% of the responding organizations were attacked by malicious software and the security issues showed an average loss of over $234,244/organization.

As indicated in Table 5.14, in WSS, although students from both faculties gave good opinions toward Web Security & Social Engineering (WSS), it is interesting to note that they considered different technical characteristics. Students from faculty of engineering considered the most the characteristic “To be able to do shopping in a secure way via Internet” (M=4.37, SD=1.06), this is because “To be able to use the necessary precautions while using interactive banking on the Internet” (M=3.93, SD=1.19). They also considered “To be able to use the necessary precautions against hoax e-mails” (M=3.89, SD=1.13) high because of “To be able to protect myself from social engineering attacks via e-mails” (M=3.61, SD=1.24). In a similar fashion, from the survey questionnaire, there were technical characteristics and differences that engineering students did not consider much. The least considered characteristic that students from engineering faculty did not consider were “To be able to take the necessary security precautions against spam e-mails” (M=3.48, SD=1.28). Faculty of Arts students did not considered “To be able to use the necessary precautions while using interactive banking on the Internet” (M=3.34, SD=1.56) much, because “To be able to do shopping in a secure way via Internet” (M=2.96, SD=1.17). “It was assumes that the reason of this difference is probably because faculties have structural differences between themselves even though they are all computer users.

Carey et al. (2014) cited that social engineering most times take the form of blackmail, trickery, impersonation when used to attack computer information systems. In these types of attacks, illegal people basically move as some kind of trusted source as a system official in order to steal personal information from innocent clients.

According to the Table 5.14, in CS although students from both faculties gave good opinions toward Computer Security (CS), it is interesting to note that they considered different technical characteristics. Students from faculty of engineering considered the most the characteristic “To be able to update a password to my files” (M=3.97, SD=1.21). That is because “To be able to add a password to my operating Windows system” (M=3.63, SD=1.25). In a similar fashion, when the survey questionnaire, there were technical characteristics and differences that engineering students did not consider much. The least considered characteristic that students from engineering faculty did not consider were “To be able to protect my personal files” (M=3.50, SD=1.28). Finally, students from the Art faculty is not considered the characteristic “To be able to protect my personal files”

(M=3.16, SD=1.33), that is because “To be able to add a password to my files” (M=3.15, SD=1.34) was not considered much. It was assumes that the reason of this difference is probably because faculties have structural differences between themselves even though they are all computer users.

Wall et al. (2013) expressed that computer security is progressively vital to associations, as security ruptures are unreasonable. Specialized security controls are not adequate to forestall security breaks, especially ruptures by workers (Wall et al., 2013). Workers are critical to keeping up secure IS (Bulgurcu et al. 2010; Crossler et al. 2013; Posey et al. 2013); be that as it may, representatives are regularly a feeble connection in securing authoritative data and IS (Willison et al. 2013). Damage by representatives, for example, information burglary and information control, cause direct damages to associations (Warkentin et al., 2013). Further, careless practices, for example, neglecting to log out of hierarchical frameworks or sharing passwords, make vulnerabilities and open doors for outside ruptures (Wall et al., 2013). Associations create security controls to deflect destructive self-sufficient activity and empower useful self-sufficient activity in workers. Sanctions, for instance, are utilized to deflect rowdiness (D’Arcy et al., 2011), while preparing and instructions are utilized to advance positive security conduct (Puhakainen et al., 2010). The significance of computer security in associations has provoked an expanding of examination on representative consistence and resistance with security polices and norms (Wall et al., 2013).

Table 5.14: Distribution of students' perception towards computer and Internet security in FOE & FOA

Security on Social Networking Sites	FOE		FOA	
	Mean	SD	Mean	SD
1. To be able to hide the information that I share on social networking sites from people.	3.97	0.99	2.48	1.25
2. To be able to block requests from people I don't know/want on social networking sites.	3.66	1.12	3.12	1.13
3. To be able to hide my profile information from people I don't want on social networking sites.	4.09	1.28	3.82	1.18
4. To be able to protect personal information I share with people on social networking sites.	3.61	1.27	2.92	1.26
5. To be able to contact the necessary people if my password is taken by someone on social networking sites	3.47	1.23	3.87	1.32
6. To be able to share videos and photos on social networking sites that will not harm my reputation.	3.47	1.24	3.89	1.32
7. To be able to share information about others on social networking sites that will not harm their reputation.	3.94	1.22	3.41	1.44
8. To be able to use social networking sites like Facebook and Twitter in a safe way.	3.73	1.23	3.40	1.30
9. To be able to protect myself from infected videos on social networking sites.	4.01	1.02	3.88	1.32
10. To be able to take necessary safety precautions against security breaches on social networking sites.	3.76	1.14	3.25	1.48
11. To be able to prevent theft of personal photo albums on social networking sites.	3.45	1.25	3.39	1.33
12. To be able to create a secure password on social networking sites.	3.46	1.24	3.37	1.35
Malicious Software				
13. To be able to prevent harmful software from infecting your computer.	4.58	0.79	2.80	1.21
14. To be able to protect my password from key loggers.	3.47	1.29	3.28	1.33
15. To be able to clean my computer when it has been infected with viruses.	3.80	1.17	3.15	1.36
16. To be able to prevent viruses from entering my computer.	3.70	1.15	3.36	1.49
17. To be able to take the necessary precautions to prevent Trojan horses from entering my computer.	4.13	1.05	3.03	1.49
18. To be able to protect my computer from worms.	4.09	0.92	2.65	1.35

Table 5.14: continued …

19. To be able to protect myself from spyware software.	3.78	1.17	3.29	1.43
20. To be able to create a very secure password.	3.80	1.17	3.18	1.37
21. To be able to use Microsoft Security Essentials.	3.78	1.15	2.68	1.20
Web Security & Social Engineering				
22. To be able to do shopping in a secure way via Internet.	4.37	1.06	2.96	1.17
23. To be able to take the necessary security precautions against spam e-mails.	3.48	1.28	3.20	1.37
24. To be able to protect myself from built-in camera pens and glasses from social engineering attacks.	3.65	1.24	3.44	1.35
25. To be able to protect myself from social engineering attacks via e-mails.	3.61	1.23	3.55	1.43
26. To be able to use the necessary precautions while using interactive banking on the Internet.	3.93	1.19	3.34	1.56
27. To be able to use the necessary precautions against hoax e-mails.	3.89	1.13	2.86	1.31
28. To be able to protect myself from phishing e-mails.	3.68	1.25	3.46	1.37
29. To be able to show the difference between HTTP and HTTPS.	3.76	1.16	3.13	1.47
Computer Security				
30. To be able to protect my personal files.	3.50	1.28	3.16	1.33
31. To be able to take the necessary security measures for logging on to my computer.	3.66	1.21	3.41	1.39
32. To be able to add a password to my operating Windows system.	3.63	1.25	3.50	1.37
33. To be able to update my security files.	3.97	1.21	3.28	1.43
34. To be able to add a password to my files.	3.81	1.18	3.15	1.34
35. To be able to create backup files in case of problems.	3.69	1.24	3.44	1.38

Where; Faculty of Engineering (FOE), Faculty of Art (FOA): Total sampled population (N); Standard Deviation (SD)

CHAPTER 6
CONCLUSION AND RECOMMENDATIONS

6.1 Conclusion

Day by day the Internet is being used more frequently. And our computer and personal files may not be completely be secure, however ability for students to use their computer and Internet safely will avert hacking if not totally but to a great height.

The results show that more students spend about 4-5 hours daily on the Internet. More students use the Internet for social media purposes. Majority of the students sampled from both faculties make use of anti-virus. there was impact of gender concerning the self-efficacy and user's perception towards computer and Internet security; that there was impact of faculties concerning the self-efficacy and user's perception towards computer and Internet security and that there was impact of age concerning the self-efficacy and user's perception towards computer and Internet security.

It was found out that there exists significant difference between SNS, MS, and WSS in both male and female students. But on the other hand, looking at the results of Computer security, there is no statistically significant difference between genders. It was found out that Male students had higher means values in SNS, MS, WSS than female students but in CS the means differences was very close and there is no significantly different between male and female students in CS.

It was found out that in SNS there existed significant difference between age 18-20 with 27+ but there are no significant differences between age 18-20 with 21-23 and 24-26. There existed no significant differences between age 21-23 with 18-20, 24-26 and 27+. There existed significant difference between age 24-26 with 27+ but there are no significant differences between age 24-26 with 18-20 and 21-23. There existed significant difference between age 27+ with 18-20 and 24-26 but there are no significant differences between age 27+ and 21-23. It was found out that in MS, there existed significant difference between age 18-20 with 27+ but there are no significant differences between age

18-20 with 21-23 and 24-26. There existed significant differences between age 21-23 with 27+ but there are no significant differences between 21-23 with 18-20 and 24-26. There existed significant difference between age 24-26 with 27+ but there are no significant differences between age 24-26 with 18-20 and 21-23. There existed significant difference between age 27+ with 18-20, 21-23 and 24-26.

It was found out that in WSS, there existed significant difference between age 18-20 with 27+ but there are no significant differences between age 18-20 with 21-23 and 24-26. There existed significant differences between age 21-23 with 27+ but there are no significant differences between 21-23 with 18-20 and 24-26. There existed no significant difference between age 24-26 with 18-20, 21-23 and 27+. There existed significant difference between age 27+ with 18-20, 21-23 and 24-26. It was found out that in CS, there is no significant difference in all age groups. It was found out that there existed significant difference between SNS, MS, and WSS in both Faculties.

It was found out that Faculty of engineering students had higher mean scores means values in SNS, MS, WSS and CS than faculty of art students. It was found out that in all groups age category 27+ had the highest total mean values and it is significantly difference from every other age group in all question category. It was found out that Male students had higher total means values than female students and there are statistically significant differences between genders in this study. It was found out that Faculty of engineering students had higher total means values than faculty of art and there are statistically significant differences between both faculty towards computer and Internet security.

From this study, it could be deducted that the results of this study will be of valuable help to the students, parents and most probably the government or universities to know the possible weakness of students’ knowledge of computer security issues and help propose a possible solution that will help salvage this problem.

6.2. Recommendations

Future research directions for the safe use of computer and the Internet security may include the following:

It is obvious that technology solutions alone are not enough and Internet security cannot be ignored. Students play important roles prior to security attitude and these calls for more studies on the variables that cause student's decision to practice Internet security. This study has shown the various factors that cause students to use computer safely. Hence, there should more awareness on Internet security to all levels of students irrespective of their faculties, and further work should be look into this subject area.

Using the same scale and collect data from other universities in north Iraq, so it will give a chance to the researcher to create a frame work for the whole north of Iraq.

Conduct the same research in a different country.

REFERENCES

Abbitt, J.T. & Klett, M.D. (2007). Identifying influences on attitudes and self-efficacy beliefs towards technology integration among pre-service educators, *Electronic Journal for the Integration of Technology in Education*, *6*, 28-42.

Abedalaziz, N., Jamaluddin, S., Chin, H.L. (2013). Measuring attitude about ICT among postgraduate students in Malaysia. *Turkish Online Journal of Educational Technology, 12*(2), 200– 216.

Abele, A. E. & Spurk, D. (2009). The longitudinal impact of self-efficacy and career goals on objective and subjective career success. *Journal of Vocational Behavior, 74*(1), 53-62.

Aboud, S. J. (2012). An Overview of Cybercrime in Iraq. *The Research Bulletin of Jordan ACM*, *2*(2), 31-34.

Abrams, M. D., & Podell, H. J. (2012). Malicious Software. *Information Security.* 111-125.

Al-Salloum, Z. S. & Wolthusen, S. D. (2010). A link-layer-based self-replicating vulnerability discovery agent. *The IEEE symposium on Computers and Communications*,*6,* 704-710.

Anderson, K. J. (2010). Internet use among college students: An exploratory study. *Journal of American College Health, 50,* 21-26.

Anderson, R. (2008). Security Engineering, (2nd ed.) New York, NY: John Wiley and Sons.

Andreassen, C. S., Torsheim, T., Brunborg, G. S., & Pallesen, S. (2012). Development of a Facebook addiction scale. *Psychological Reports,110*(2), 501–517.

Ayub, A. F. M., Hamid, W. H. W., & Nawawi, M. H. (2014). Use of Internet for academic purposes among students in Malaysian institutions of higher education. *The Turkish Online Journal of Educational Technology*, *13*(1), 232-241.

Baaij, E. (2012). *Safe Internet Use How a Website Can Stimulate Internet Safety* (Master Thesis). Retrieved from Philosophy of Science, Technology and Society Science and Technology Studies, 1-58.

Bagachi, K. & Udo G. (2003) An analysis of the growth of computer and Internet security breaches, *Communications of the AIS, 12*, 684-700.

Bandura, A. (1997). *Self-efficacy: The Exercise of Control*, Freeman, New York, NY.

Baron, L. & Morin L. (2010). The impact of executive coaching on self-efficacy related to management soft-skills. *Leadership and Organization Development Journal, 31*(1), 18-38.

Bebetsosi, E. & Antoniou, P. (2009) Gender differences on attitudes, computer use and physical activity among Greek university students. *The Turkish Online Journal of Educational Technology, 8*(2), 63-67.

BigPlanet (2010). Understanding Internet security - what you need to protect yourself online. *Internet Security,* 1-14.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness, *MIS Quarterly, 34*(3), 523-548.

Carey, D., Misch, A., Spencer, A. & Speranza, R. (2014). Self-Disclosure on Social Networking Sites. In partial fulfillment of the Interactive Qualifying Project. Worcester Polytechnic Institute, 1-82.

Carroll, A., Houghton, S., Wood, R., Unsworth, K., Hattie, J., Gordon, L., Bower, J. (2009). Self-efficacy and academic achievement in Australian high school students: the mediating effects of academic aspirations and delinquency. *Journal of Adolescence, 32* (4), 797- 817.

Carruth, K. A., & Ginsburg, H. J. (2014). Social networking and privacy attitudes among college students. *Psychology, Society, and Education*, *6*(2), 82-93.

Cavus, N., & Ercag, E. (2014). 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, 46*(6), 1-15.

Chen, J., Paik, M., & McCabe, K. (2014). Exploring Internet security perceptions and practices in Urban Ghana. *Symposium on Usable Privacy and Security,* Menlo Park, CA, 1-14.

Citron, D.K. (2010). *Civil rights in our information age, in the offensive Internet*edited by S. Levmore and M.C. Nussbaum, Harvard University Press, 31-49.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers and Security*, *32*, 90-101.

Cyr, D., Head, M., & Larios, H. (2010). Colour appeal in website design within and across cultures: A multi-method evaluation. *International Journal of Human-Computer Studies*, *68*(1), 1–21.

D’Arcy, J., & Herath, T. (2011). A review and analysis of deterrence theory in the IS security literature: Making sense of the disparate findings. *European Journal of Information Systems, 20*, 643-658.

D’Arcy, J., Hovav, A. & Galletta, D. F. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach,*Information Systems Research, 20*(1), 79-98.

Egbo et al (2011). Gender perception and attitude towards eLearning: a case of business students. *International Journal of Computer Application, 2*(1), 135-148.

Enrici, I., Ancilli, M., & Lioy, A. (2010). A psychological approach to information technology security. *3rd International Conference on Human System Interaction*, Rzeszow, Poland: 459–466.

Geniş-Gruber, A., Gönül, M. S. & Taş, B. K. O. (2012). Obstacles to online shopping: Impact of gender and Internet security issues. *Dokuz Eylül Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, *27*(2), 27-54.

Guy, R. S. & Jackson, L. M. (2010). An examination of undergraduates’ self-efficacy beliefs and demonstrated computer skills. *Issues in Informing Science and Information Technology, 7*, 12-16.

Hachman, M. (2012). Anonymous: Symantec offered $50K for stolen code, plus a lie, *PC Magazine.* Retrieved from: http://www.pcmag.com/article2/0,2817,2399912,00.asp.

Hauser, R., Paul, R., & Bradley, J. (2012). Computer self-efficacy, anxiety, and learning in online versus face to face medium. *Journal of Information Technology EducationResearch,11*, 142-154.

Hayashi, E., and Hong, J. I. (2011). A diary study of password usage in daily life, *in Proceedings of the 29th Annual Conference on Human Factors in Computing Systems*, Vancouver, BC, Canada.

Herley, C. (2010). So long, and no thanks for the externalities: the rational rejection of security advice by users. *In Proceedings of the 2010 Workshop on New Security Paradigms Workshop. ACM,* 133–144.

Howe, A. E., Ray, I., Roberts, M., Urbanska, M., Byrne, Z. (2012). The psychology of security for the home computer user. *IEEE Symposium on Security and Privacy.* 209-233.

Hsiao, H., Tu, Y. and Chung, H. (2012). Perceived social supports, computer self-efficacy, and computer use among high school students*: The Turkish Online Journal of Educational Technology, 11*(2), 167-177.

Huang, C. (2010). Internet use and psychological well-being: A meta-analysis. Cyber-psychology. *Behavior and Social Networking,13*(3), 241–249.

Jelenchick, L. A., Eickhoff, J. C., & Moreno, M. A. (2013). Facebook depression? social networking site use and depression in older adolescents. *The Journal of Adolescent Health: Official Publication of the Society for Adolescent Medicine*, *52*(1), 128–130.

Kim, J., & Lee, J. E. R. (2011). The Facebook paths to happiness: Effects of the number of Facebook friends and self-presentation on subjective well-being. *Cyberpsychology Behavior and Social Networking,14*(6), 359–364.

Kim, T. H.-J., Bauer, L., Newsome, J., Perrig, A., &Walker, J. (2010). Challenges in access right assignment for secure home networks. *In Proceedings of 5th USENIX Workshop on Hot Topics in Security,* Washington, DC, USA.

Kirat, D., Vigna, G., & Kruegel, C. (2014). Barecloud: bare-metal analysis-based evasive malware detection. ACM,*7*, 287-301

Kross, E., Verduyn, P., Demiralp, E., Park, J., Lee, D. S., Lin, N., et al. (2013). Facebook use predicts declines in subjective well-being in young adults. *PLoS ONE,8*(8), 12-24.

Kuss, D. J., & Griffiths, M. D. (2011). Online social networking and addiction – A review of the psychological literature. *International Journal of Environmental Research and Public Health, 8*(9), 3528–3552.

Lee, M.H. & Tsai, C.C. (2010).Exploring teachers' perceived self-efficacy and technological pedagogical content knowledge with respect to educational use of the World Wide Web. *Instructional Science,38*, 1-21.

Liang, H. &Xue, Y. (2010). East Carolina understanding security behaviors in personal computer usage: A Threat Avoidance Perspective. *Journal of the Association for Information Systems,11*(7), 394-413.

Liaw, S. S., &Huang, H. M. (2011). A study of investigating learners attitudes toward e-learning. *5th International Conference on Distance Learning and Education*, 28-32.

Lindgaard, G., Dudek, C., Sen, D., Sumegi, L., &Noonan, P. (2011). An exploration of relations between visual appeal, trustworthiness and perceived usability of homepages. *ACM Transactions on Computer-Human Interaction,18*(1), 1.

Litterell, A.B., Zagumny, M.J. & Zagumny, L.L. (2005). Contextual and psychological predictors of instructional technology use in rural classrooms. *Educational Research Quarterly, 29*(2), 37-47.

Liu, C.-Y., & Yu, C.-P. (2013). Can Facebook use induce well-being? cyberpsychology, behavior and social networking, *16*(9), 674–678.

Mahajan, P. (2009). Use of social networking in a linguistically and culturally rich India. *International Information and Library Review*, *41*, 129–136.

Madhavan, P. & Phillips, R. R. (2010). Effects of computer self-efficacy and system reliability on user interaction with decision support systems. *Computers in Human Behavior, 26*(2), 199-204.

Maimunah, M. S., Roshidi, H. &Roslani, E. (2012). Technology acceptance and computer anxiety. *International Conference on Innovation, Management and Technology Research*, Malacca, Malaysia.

Maimunah Roshidi, M. S. H., and Roslani, E. (2011). Technological changes and its relationship with computer anxiety in commercial Banks. *The 2nd International Research Symposium in Service Management* Yogyakarta, Indonesia. Yogyakarta, Indonesia.

Mekovec, R., &Hutinski, Z. (2010). The role of perceived privacy and perceived security in online market. *MIPRO 2012/ISS*, 1883-1888.

Monsuwe, T. P., Dellaert, B. and Ruyter, K. (2004). What drives consumers to shop online A literature review.*International Journal of Service Industry Management, 15*(1), 102-121.

Murphy, C.A., Coover, D. & Owen, S.V. (1989). Development and validation of the computer self-efficacy scale. *Educational and Psychological Measurement*, *49,* 893-899.

Ng, B-Y. &Rahim, M. A. (2010). A socio-behavioral study of home computer users' intention to practice security. *Pacific Asia Conference on Information Systems*, 1-14.

O'Keeffe, G. S., & Clarke-Pearson, K. (2011). The impact of social media on children, adolescents, and families. *Pediatrics,127*(4), 800-804.

Odell, P., Korgan, K., Schumachere, P., &Delucchi, M. (2010). Internet use among female and male college students. *Cyber Psychology and Behavior, 3*(5), 855-862.

Orchard, L. J., Fullwood, C., Galbraith, N., & Morris, N. (2014). Individual differences as predictors of social networking. *Journal of Computer-Mediated Communication,4*, 12-19.

Owusu, E., Han, J., Das, S., Perrig, A.,&Zhang, J. (2012).Accessory: password inference using accelerometers on smartphones. *Proceedings of the Thirteenth Workshop on Mobile Computing Systems and Applications*. *ACM.7*, 12-34.

Posey, C., Roberts, T. L., Lowry, P. B., Bennett, R. J., and Courtney, J. (2013). Insiders' protection of organizational information assets: Development of a systematics-based taxonomy and theory of diversity for protection-motivated behaviors. *MIS Quarterly, 12*, 23-29.

Puhakainen, P., &Siponen, M. (2010). Improving employees' compliance through information systems security training: an action research study. *MIS Quarterly,34*(4), 757-778.

Reinecke, L., & Trepte, S. (2014). Authenticity and well-being on social network sites: A two-wave longitudinal study on the effects of online authenticity and the positivity bias in SNS communication. *Computers in Human Behavior,30*, 95–102.

Salleh, N., Hussein, U. &Aditiawarman, R. (2011). Information disclosure behavior in social media among Malaysian Youth: The impact of privacy concern, risk and trust. *Symposium on Information and Computer Sciences*, 1-4.

Sam, H. K., Othman, A. E. A., &Nordin, Z. S. (2005). Computer self-efficacy, computer anxiety, and attitudes toward the Internet: A study among undergraduates in UNIMAS. *Educational Technology and Society*, *8*(4), 205-219.

Saprikis, V., Chouliara, A., &Vlachopoulou, V. (2010). Perceptions towards online Shopping: Analyzing the Greek university students attitude. *Communications of the IBIMA*, 1-13.

Scott, J. E. (2010). Measuring dimensions of perceived e-business risks. *Information Systems and e-Business Management, 2*, 31-55.

Shin, D.-H., & Shin, Y.-J. (2011). Why do people play social network games? *Computers in Human Behavior,27*(2), 852–861.

Shukla, J.B., Singh, G., Shukla, P., and Tripathi, A. (2014). Modeling and analysis of the effects of antivirus software on an infected computer network. *Applied Mathematics and Computation, 227,* 11–18.

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

Stephen J. Cutler, Hendricks, J. &Guyer, A. (2003). Age differences in home computer availability and use. *Journal of Gerontology*: *58B*(5), S271–S280.

Suri, G. &Sharma, S. (2013). The impact of gender on attitude towards computer technology and e-learning: An exploratory study of Punjab university, India. *International Journal of Engineering Research,2*(2), 132-136.

Suri, G., Navkiran, Kaur, G. &Sharma, S. (2014). Gender influence in e-learning Platforms: an exploratory study of Punjabi university, Patiala, India. *SPC ERA IJBM*, *2*(6), 77-85.

Teo, T., & Koh, J. H. L. (2010). Assessing the dimensionality of computer self-efficacy among pre-service teachers in Singapore: A structural equation modeling approach. *International Journal of Education and Development using Information and Communication Technology,6*(3), 7-18.

Valkenburg, P. M., & Peter, J. (2009). Social consequences of the Internet for adolescents: A decade of research. *Current Directions in Psychological Science,18*(1), 1–5.

Valkenburg, P. M., Peter, J., &Schouten, A. P. (2006). Friend networking sites and their relationship to adolescents' well-being and social self-esteem. *CyberPsychology and Behavior,9*(5), 584–590.

Wall, J. D., Palvia, P. &Lowry, P. B. (2013). Control-related motivations and information security policy compliance: The role of autonomy and efficacy. *Issues in Information Security Policy Compliance,9*(4) 52-79.

Wash, R. (2010). Folk models of home computer security. In Proceedings of the Sixth Symposium on Usable Privacy and Security, *ACM*, 11.

Willison, R., &Warkentin, M. (2013). Beyond deterrence: An expanded view of employee computer abuse, *MIS Quarterly,37*(1), 1-20.

Zhao, Y., Pugh, K., Sheldon, S. & Byers, J.L. (2002). Conditions for classroom technology innovations. *Teachers College Record,104*(3), 482-515.

APPENDICES

Appendix

SCALE FOR SELF-EFFICACY AND PERCEPTIONS IN THE SAFE USE OF THE INTERNET

The questionnaire aim to define your understand and opinions on self-efficacy and user's perception towards computer and Internet security. You are kindly expected to choose the best answer that you feel is closet to. The result of this questionnaire will solely be used for the analysis in the research report, and will not be provided to any institution in any way.

Thanks in advance for taking time to answer our questionnaire.

Assoc. Prof. Dr. Nadire Cavus
Didar Dlshad HAMAD AMEEN (Master Student)

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

1) **Gender** □ Male □ Female

2) **Age** □18-20 □ 21-23 □ 24-26 □27+

3) **Faculty**: □Art □Engineering

4) **Class (year):** □1 □2 □ 3 □ 4 □ 5+

5) **Academic position :** □ Undergraduate □ Postgraduate

SECTION II: Internet Usage

6) **How many hours do you spend on INTERNET in an everyday?**

□ 0-1 □ 2-3 □ 4-5 □ 6+

7) **For what reason do you use the INTERNET**(you can choose more than one option)

□Online banking

□E-learning

□ E-commerce

□ E-government

□ Social media (Facebook, twitter… etc.)

□ Emails

□ Online shopping

8) Do you have anti-virus program in your computer?

□ Yes □ No

SECTION III: Scale for Self-Efficacy and Perceptions in the Safe use of the Internet (please tick the most appropriate to you)

Items	**Very Confident**	**Confident**	**Neutral**	**Not confident**	**Not Very Confident**
Security on Social Networking Sites					
1. To be able to hide the information that I share on social networking sites from people.					
2. To be able to block requests from people I don't know/want on social networking sites.					
3. To be able to hide my profile information from people I don't want on social networking sites.					
4. To be able to protect personal information I share with people on social networking sites.					
5. To be able to contact the necessary people if my password is taken by someone on social networking sites					
6. To be able to share videos and photos on social networking sites that will not harm my reputation.					
7. To be able to share information about others on social networking sites that will not harm their reputation.					
8. To be able to use social networking sites like Facebook and Twitter in a safe way.					
9. To be able to protect myself from infected videos on social networking sites.					
10. To be able to take necessary safety precautions against security breaches on social networking sites.					
11. To be able to prevent theft of personal photo albums on social networking sites.					
12. To be able to create a secure password on social networking sites.					
Malicious Software					

13. To be able to prevent harmful software from infecting your computer.					
14. To be able to protect my password from key loggers.					
15. To be able to clean my computer when it has been infected with viruses.					
16. To be able to prevent viruses from entering my computer.					
17. To be able to take the necessary precautions to prevent Trojan horses from entering my computer.					
18. To be able to protect my computer from worms.					
19. To be able to protect myself from spyware software.					
20. To be able to create a very secure password.					
21. To be able to use Microsoft Security Essentials.					
Web Security & Social Engineering					
22. To be able to do shopping in a secure way via Internet.					
23. To be able to take the necessary security precautions against spam e-mails.					
24. To be able to protect myself from built-in camera pens and glasses from social engineering attacks.					
25. To be able to protect myself from social engineering attacks via e-mails.					
26. To be able to use the necessary precautions while using interactive banking on the Internet.					
27. To be able to use the necessary precautions against hoax e-mails.					
28. To be able to protect myself from phishing e-mails.					
29. To be able to show the difference between HTTP and HTTPS.					
Computer Security					
30. To be able to protect my personal files.					
31. To be able to take the necessary security measures for logging on to my computer.					
32. To be able to add a password to my operating Windows system.					
33. To be able to update my security files.					
34. To be able to add a password to my files.					
35. To be able to create backup files in case of problems.					