THE REPUBLIC OF TURKEY
BAHCESEHIR UNIVERSITY

MEASURING THE CYBER SECURITY AWARENESS OF UNIVERSITY STUDENTS

Master's Thesis

ASMA'U MUKTAR ALIYU

ISTANBUL, 2015

THE REPUBLIC OF TURKEY
BAHCESEHIR UNIVERSITY

THE GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES
INFORMATION TECHNOLOGY

MEASURING THE CYBER SECURITY AWARENESS OF UNIVERSITY STUDENTS

Master's Thesis

ASMA'U MUKTAR ALIYU

Advisor: Asst.Prof.Dr. Dilek KARAHOCA

ISTANBUL, 2015

THE REPUBLIC OF TURKEY
BAHCESEHIR UNIVERSITY

THE GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES
INFORMATION TECHNOLOGY

Name of the thesis: Measuring the Cyber Security Awareness of University Students

Name/Last Name of the Student: Asma'u Muktar Aliyu

Date of the Defense of Thesis: 22.05.2015

The thesis has been approved by the Graduate School of Natural and Applied Sciences.

Assoc.Prof.Dr. Nafiz ARICA
Graduate School Director

I certify that this thesis meets all the requirements as a thesis for the degree of Master of Arts.

Prof. Dr. Adem KARAHOCA
Program Coordinator

This is to certify that we have read this thesis and we find it fully adequate in scope, quality and content, as a thesis for the degree of Master of Arts.

Examining Committee Members Signature

Thesis Supervisor
Asst.Prof.Dr. Dilek KARAHOCA

Member
Prof. Dr. Adem KARAHOCA

Member
Prof.Dr. İbrahim PINAR

ACKNOWLEDGEMENT

I would like to thank my mother and father, Mr & Mrs Muktar Aliyu for their support, my sisters and my brother for always choosing to believe in me.
I would also like to thank my advisor and supervisors Prof. Dr Adem Karahoca & Assist. Prof. Dr Dilek Karahoca for helping me through out my masters program and my thesis and also for always nudging me in the right direction.

Istanbul, 2015 Asma'u Muktar Aliyu

ABSTRACT

MEASURING THE CYBER SECURITY AWARENESS OF UNIVERSITY STUDENTS

Asma'u Muktar Aliyu

Information Technology

Thesis Supervisor: Asst. Prof. Dr. Dilek Karahoca

May 2015, 90 Pages

This thesis explores the awareness level of university students regarding cyber security. It explores the major risks that students face in terms of information security and how their social cognitive behaviors affect their cyber activities. It also gives background information regarding information security, how security is compromised, who a hacker is, how they think and what we can do to protect ourselves from malicious activities that lurk around the virtual space. A survey was carried out to test university students' level of awareness. The results from this survey were used to tally the overall results of students and come up with a conclusion on the risks and vulnerabilities that students are likely to face.

Keywords: Cyber Security, Information Security, Hacking, Security Risks, Social Cognitive Behaviour.

ÖZET

ÜNİVERSİTE ÖĞRENCİLERİNİN SİBER GÜVENLİK FARKINDALIĞININ ÖLÇÜLMESİ

Asma'u Muktar Aliyu

Bilgi Teknologi

Tez Danışmanı: Assist. Prof. Dr, Dilek Karahoca

May 2015, 90 Sayfalar

Bu tez siber güvenlik konusunda Üniversite öğrencilerinin farkındalık düzeyini araştırmaktadır. Öğrencilerin bilgi güvenliği açısından karşılaştıkları temel risklerin, sosyal bilişsel davranışlarının, siber faaliyetleri nasıl etkilediğini de incelemektedir. Ayrıca çalışmada, bilgi güvenliğinde güvenlik nasıl tehlikeye düşer, haker kimdir, nasıl düşünürler ve sanal alemde pusudan ve zararlı faaliyetlerden kendimizi korumak için ne yapabiliriz gibi konularda da bilgi verilmektedir. Bir anket uygulanarak üniversite öğrencilerinin siber günvenlik konusundaki farkındalığı analiz edilmeye çalışıldı. Bu araştırmanın sonuçları, öğrencilerin genelde siber güvenlik konusundaki farkındalıkları incelendi.

Anahtar Kelimeler: Siber Güvenlik, Bilgi Güvenliği, Siber Saldırılar, Güvenlik Riskleri, Sosyal Bilişsel Davranış.

CONTENT

LIST OF TABLES

LIST OF FIGURE

LIST OF SYMBOLS

CSV: Comma-separated values

DNS: Domain Name System

FTP: File Transfer Protoco

HTTP: Hypertext Transfer Protocol

IBM: International Business Machines

IS: Informaation Security

IP: Internet Protocol

P2P: Peer-To-Peer, Peer-2-Peer

SCT: Social Cognitive Theory

SEIS: Self Efficacy in Information Security

SPSS: Statistical Package for the Social Sciences

SYN-ACK: Synchronize and Acknowledge

TTL: Time To Live

1. INTRODUCTION

Cyber security also known as Network security or IT security is information/data security that concerns digital/computing devices like smartphones, computers (pcs, networks), servers and also Internet. Cyber security covers all elements of computer/network security that protects devices from unauthorized access, change and destruction of information systems. With the widespread of computer usage and Internet reliance, cyber security is an important part of any information system.

Cyber security vulnerabilities are the components that put a system or network at risk of getting infected with malicious software. The term vulnerability means features of a system that render it helpless against an intentional assault or unsafe circumstance. This term originates from the Latin word vulnus—wound and the comparing verb vulnero—to harm, wound, damage, hurt. The term vulnerability is a sample of precarious circumstances where the dialect makes it simple to make a valuable word through the procedure known as objectification, which refers to a few natural circumstances, yet the general degree, of which is not exactly as clear. When one realizes that a system was affected by an assault, this means that an assault on the framework occurred and succeeded. It can be presumed that the system was powerless against the assault, then the expression vulnerability can be utilized to refer to the peculiarities of the framework that made it defenseless against the assault or to refer to the gimmicks of all frameworks that make them helpless against a comparable assault, or to refer to peculiarities of all frameworks that make them helpless against all assaults (Mansourov, Campara, 2010).

Even with new systems been created everyday, systems that are said to be impenetrable and completely safe from outside/inside assaults still fall victims of cyber attacks, systems vulnerabilities are still exploited. The rising rate of cyber crime is still so rampant among citizens that Americans are more afraid of a cyber war than they are afraid of Iranian, North Korean nuclear weapons and also Climate change. Network security is a huge referent question yet its political significance emerges from associations with the aggregate referent articles of “The State”, “The Society”, “The Nation” and “The Economy” (Singer, Friedman (2013). Malwares are used all over internet services to affect devices daily and carry out assaults that render devices,

networks and data vulnerable. The Osterman research survey found out that eleven million malware variations were found by 2008 and ninety percent of these malware originated from concealed downloads from prominent and trusted sites (Osterman Research Survey). Before a download happens, a client is initially needed to visit the malevolent webpage. To bait the client into going by a site with vindictive substance, hackers would send out spam messages that contain various connections to the site. When clueless client visits the pernicious site, malware is downloaded and introduced in the victimized person's machine/network without the client figuring out what is going on. For instance, the notorious Storm worm which makes utilization of its own system, numerous of tainted PCs to send spam messages containing connections to malicious web pages.

1.1 RESEARCH QUESTION AND OBJECTIVES

This thesis focuses on students and their knowledge of IS. The aim is to measure the Information Security awareness level amongst university students. Online security, which is a pressing matter in a society that has become a global village, is an issue that must be at the forefront of every educational system so as to secure the safety of young people within cyber environments. The research question, which this thesis focuses on is, *how much do students know about information security and what can be done to make sure students remain safe in online communities*. Since there is not much IS awareness programs available for students globally, this thesis will explore the existing IS awareness programs available to students. It will also perform an in-depth survey in which students from different universities around the world answer a questionnaire that asks questions about their basic online behaviors. This will be used to determine the IS awareness level of students and what factors influence the awareness level of students. This thesis will also come up with a number of hypotheses (such as age, gender) that could be determinant factors in measuring the awareness level of students and perform an analysis to prove these hypotheses.

Research Step One: To measure the awareness level of students based on the results of questions answered in the questionnaire and the risks students face.

Research Step Two: To explore, based on the hypotheses what factors affect the awareness level of students.

The aim of *research step one* is to measure the awareness level of students and understand what it means. In the post-survey analysis, there will be a hierarchy grouping of the, which will be used to understand the analysis proceedings.

The aim of *research step two* is to prove, using a statistical analysis tool, the hypotheses brought forward in this paper. The analysis tool will tally the results of the survey which will provide an insight to what it is that affects students and determines what kinds of students have a working knowledge of IS.

1.2 THESIS STRUCTURE

The first section of this thesis discusses the fundamentals of cyber security, it gives a general insights about IS, how security is compromised and what we can do about our online safety and examples of how security has been compromised before, what methods were used and also types of risks and counter measures. A literary review, which is an analyses the theory of planned behavior (Icek Ajzen) and how it can be used to measure and understand the IS awareness levels/online safety precautions of students. The second section discusses the materials that will be used to come up with the findings for this thesis. It discusses the survey, which will be carried out and the statistical analysis process. A pre-test and post-test survey was carried out to ensure the accuracy of the results discussed in this paper. Section three of this paper discusses the findings from the survey questionnaire. It discusses the risk level of the students, i.e. how much of a risk is posed towards students and also tries to answer the main research question in this thesis (*how much do students know about information security and what can be done to make sure students remain safe in online communities*.).

1.3 CYBER SECURITY FUNDAMENTALS

There are so many ways in which security of a system can be compromised. New technologies are being created everyday and new forms of security compromises are being discovered and there are also a lot of ways in which users can remain safe while traversing through the virtual environment. To understand the workings of IS and how IS compromised, a review on the methodologies that can be used to exploit security was made.

Methodologies such as authentication and authorization are used to check if a client is sure of an item. Conventional verification and approval instruments utilize three separate elements to check a user to confirm if the user has the right capacity to get to the object. The first place component is something familiar, e.g. password or an individual ID number (PIN). It makes sure that just the manager of the record who knows the password or PIN is expected to get to the record. Second element is something a user has which incorporates smart card or security token. It expects just the holder of the record to have the important smart card or token expected to open the record. Third element is something a user is, e.g. sound of the voice, unique fingerprint, or iris qualities. The authentication and authorization methodologies of securing data do not guarantee the security of a system. A system must have loopholes or vulnerable components through which the system can easily be breeched and exploited. Computer infrastructures come with some vulnerable components, which will always place a device at a risk. These components are Software, Hardware and Network. In order to secure these components, three elements must be in place. These elements include accountability, which is used for the detection of malicious elements, a perimeter defense system that is used for defense against the breach of infrastructure by malicious elements and an access control mechanism, which is used for authorization of incoming/outgoing data (Jang-Jaccard, Nepal, 2012*)*.

There are various ways in which unauthorized access can be gained to any computing system. These unauthorized access are malicious activities, specially created to gain entry into a system through various means. There are several methods of compromising (commonly known as hacking) a system, some of these methods are: Malware, Denial-of-

Service, Backdoors, Eaves Dropping, Spyware, Exploits, Direct Access Attacks, Indirect Attacks.

Malware: Malwares (malicious software) are the most common threat to Cyberspace either by exploitation of vulnerable spaces or utilization of new technologies. There are different types of malwares and several methods of spreading them to attack a system. There are Trojans, viruses, worms, bot executable, rogue ware etc. All of these malwares can be loaded into systems via opening of tainted files or via accessing of infected websites. These will get the malwares downloaded into a system hence giving access to hackers. Malwares can also be transmitted via removable USB devices. They can be loaded into a USB drive and then transmitted from one system to another.

Victims of malware attacks are, end-user systems, servers, network devices (e.g. routers, switches) and process control system such as Supervisory Data Acquisition (SCADA). Social medias ability to reach millions of users at once gives hackers and opportunity to befriend several users and send them spam mails at once hence gaining access to several computers/devices at once and compromising their security. Also, the growing trove of information stored in the cloud is attracting hackers to exploit cloud-based data and gain access to a lot of information.

Malwares evolve through time as technology evolves therefore capitalizing on emerging technologies and exploiting their flaws to avoid detection (TechTerms, 2005)

Denial-of-Service: Distributed Denial of Service (DDoS) has additionally developed over the long haul. DDoS assaults utilize multitudes of zombie machines, assume control, and are controlled by a solitary expert to overpower the assets of the victimized people's packet. These computers send multiple data packets at the same time to a target server to overwhelm and render it useless. For example in February 2000, where the most popular e-commerce websites were shut by concurrent assaults. From that point forward, the notoriety of parties associated with denial of services attacks has expanded, and the leaders of the armed forces of DDoS zombies are exploiting this popularity. They take advantage of the lack of security that the average computer user at home has, attackers have figured out how to plant dirty programming to surrender the remote control of home PCs programs. Hackers often send out DDoS attacks against a group of targets yet the threat lies in a facilitated assault of the imperative national assets, for example, communications, keeping money and budgetary goals. DDoS assaults on basic

correspondence hubs would be particularly destructive, particularly amid an emergency (Rouse, 2007)

IP Spoofing*:* Internet Protocol Spoofing (IP spoofing) is a technique used to make a PC system components communicate by adjusting the IP locations of the source component in the information parcels by supplanting them with false addresses. IP-spoofing makes a circumstance that breaks the ordinary relationship of trust that must exist between two components that communicate. IP datagrams are easy to open, view and modify allowing randomly chosen IP address to be inserted into a datagram as a legitimate source address. These conditions create opportunities for IP-spoofing by allowing a small number of certain IP addresses to be used by many communication elements. The process works as follows: a connecting element intercepts IP datagrams, opens and modifies its original IP address and then sends them through. If any other changing elements in the network should receive any of these datagrams, it maps these addresses in the IP address table as legal origin, and used for subsequent correspondence with the elements "source" with those fake addresses (Du Paul).

Spyware: Spyware is a type of malware that lodges onto computers. These soft wares have the ability to send information gathered from gaining access to a victims system from the host computer to other computers or take control of the victims' computer without their knowledge. Spywares are like Trojan horses which victims can get from downloading and installing malicious software. Spyware exists as autonomous executable projects, they find themselves able to keystrokes, yield records on the hard disk, snoop distinctive applications, e.g., chats or word processors, present other spyware ventures and afterward dependably giving off this information back to the spyware creator who will either use it for publicizing/advancing purposes, offer the information to a substitute party or for vindictive purposes (Microsoft Spyware).

Bots: Bots can be referred to as, Web robots, or www robots, are little programming that run robotized goals over the Internet. Generally they run basic assignments that the individual would some way or another not need to perform, however at a much speedier pace. At the point when they utilized noxiously, they are a sickness, surreptitiously dropped in numerous uncovered PCs (for the most part those found in homes), to stop them without their insight and transform them into slaves to split delicate information. These identify with the PCs, known as bots, they are connected to the air and typically

found in systems called botnets. Botnets are intended to work so that the command center has to come to PC and shared rapidly between different computers botted in the network. There are all kinds of Bots. There are bots that harvest email addresses (spam bots), viruses and worms, file name comparisons, automated purchase of concert tickets, and bots that work with botnets, or coordinated attacks on networked computers (Rouse 2005)

Network Intrusion: A network intrusion is an unapproved entrance into a company's system, or an individual machine address in an appointed area. Intrusions are sometimes aloof (the entrance is picked up subtly and without identification) or dynamic (changes to system assets are effected). Intrusions can originate externally from a systems structure or internally (a representative, a client, or business accomplice). A few intrusions are basically intended to tell you the interloper was there by damaging your website with different sorts of messages or unrefined pictures. Others are more vindictive, looking to concentrate basic data on either a one-time premise or as a progressing parasite like relationship that keeps on siphoning off information until it has found what it is looking for. A few gatecrashers embed deliberately made code, for example, Trojan-sort vindictive software (malware), intended to take passwords, record key- strokes, or open an application's secondary passage (Vacca 2012*)*.

Through the use of a digital watering hole cybercriminals devised a new deceptive way of scamming users. In a watering hole attack, a website known to be visited by potential victims is infected with malware, either through convincing targets to proceed to a link or through the use of undocumented zero-day exploits in order to remotely execute code on systems where access would not normally be possible. This can target a specific company or sector of industry, or can seek a mass infection of visiting internet traffic (Digital Data Communications, 2014).

1.3.1 How Security Is Compromised

There are several ways in which the security of a network can be breached. One of the following ways is when the connection between computers is established. Usually they follow these patterns of etiquette and protocols called handshake procedure. Sometimes is even referred to as triple handshake. The subnet of the target is examined by the assailant

during the first stage of infection in a botnet attack. This examination explores the targets subnet for obvious vulnerabilities. The victimized persons' machines are then tainted via a distinctive exploitative routine. This is then followed by the auxiliary injection where the hosts, which are being contaminated, execute a shell-code. This gets the genuine bots picture, which is parallel to the particular area through FTP, HTTP, or P2P. The bot is then reintroduce on to the target machine. Once this has been done, the victims' pc is then turned into a zombie machine, which then runs the malicious code. Every time the zombie machine gets rebooted, the bot application gets rebooted as well. The bot application makes a command and control channel, which interfaces the zombie machine to the command and control server. Once the command and control channel has been established, the zombie machine becomes a part of the hackers botnet armed force. The original botnets command and control exercise begin after the connection stage. The head of the bots (botmaster) will then utilize the command and control channel to scatter orders to his bot armed force. The botmaster sends orders to the bot applications, which receive and execute them. The command and control channel empowers the botmaster to remotely control the activity of an extensive amount of bots to lead different illegal exercises. Finally, the bots have to be kept alive and updated. In this final stage, the bots are ordered to retrieve a redesigned twofold. Botmasters may then need to overhaul their botnets for few cases. e.g. Bot doubles may need to be overhauled to avoid location detection methodologies. Additionally, now and again the upgraded double moves the bots to an alternate command and control server. This is called server movement; it is exceptionally for botnets to be kept alive. Botmasters attempt to make sure that their bots remain undetectable and versatile by utilizing a DDNS (Dynamic DNS). This is a resolution service, which encourages successive upgrades and changes in server areas. On the off chance that power surges disturb a command and control server at a particular IP address, an alternative command and control server can be set up by the botmaster which has the same name but at a different IP. IP location changes in C&C servers proliferate very quickly due to bots brief time-to-live (TTL) values for the space names set by DDNS suppliers. Subsequently, bots can move to the new command and control server area and can stay alive (Feily, Shahrestani, Ramadass 2009).

Part of the normal attacks that endeavor the program security can be through augmentations, frequently called "plug-in" or "add-on" and scripting dialects, for

example, JavaScript or VBScript. Extensions are components of software that are reusable, which can be connected to a program to give usefulness or to tweak a clients' experience. Anybody, with a little programming knowledge and coding skill, can add external code onto an extension and numerous clueless clients can download it unreservedly. Such augmentations regularly contain programming bugs that significantly expand the assault area for the aggressors to exploit them. The capacity to run a scripting dialect, for example, JavaScript or VBScript permits site page creators to include a lot of gimmicks and intelligence to a website page. Notwithstanding, assailants can mishandle this same ability. A remarkable helplessness of misusing scripting dialect is Cross-site Scripting (XSS). XSS empowers aggressors to infuse vindictive script into website pages. At the point when clueless customers visit the website pages, the noxious code is executed to perform malicious exercises on client's PC (Jang-Jaccard, Nepal 2012*)*.

1.3.1 The Hacking Of iCloud

It was reported that Google, Yahoo and Microsoft's Hotmail were assaulted in the same way that Apples' iCloud was assaulted. Chinas Apple iCloud capacity and reinforcement administration was assaulted by programmers attempting to take client credentials, reported a Chinese site checking association. A "man-in-the-middle" (MITM) assault was utilized. The programmers mediated their own particular site in the middle of clients and Apple's iCloud server, catching information and conceivably getting access to passwords, iMessages, photographs and contacts (Greatfire 2014).

An article reported on The Hacker News claims that, A group of Dutch-Moroccan programmers that called themselves Team DoulCi had apparently asserted to hack a defensive peculiarity on Apple's iCloud framework, that could influence an aggressor to remove the security on missing/stolen iPhones. The programmers obtained bolted iPhone gadgets for $50 to $150 and afterward skirted Apple's iCloud activation lock through a loophole in Apples security, which they have not found a way to patch up it seems. The basic vulnerability in the Apple's iCloud permitted them to open stolen iPhones in a moment, which could then be sold for a vast benefit in the Black-market. Security specialists accepted that with the utilization of this vulnerability, the programmers could

do a great deal more than simply open the stolen gadgets. Security experts trust it may be conceivable that the programmers can educate the gadgets to peruse iMessages and even force data including AppleID accreditations. It took the programmers five months to rupture Apple's iCloud framework and a Twitter account that may be connected to the same 'Doulci programmer' bunch, posted a tweet, which guarantees that the team have accessed more than 5,700 Apple gadgets in only five minutes of initiating the hack. With the great propositions and just to be on a more secure side, the group allegedly reached Apple about this helplessness back in March, yet Apple never reacted and stayed noiseless on the matter, which animated the programmers to open up to the world about the revelation. The programmers say they at last chose to approach the Dutch media on the grounds that Apple has not yet conceded openly that its system has been compromised. The pair of programmers are putting forth opening administrations by means of doulCi.nl site, as per data found on their site. DoulCi is the world's first Alternative iCloud Server, and the world's first iCloud Activation Bypass (Khandelwal 2014).

The Dutch programmer, AquaXetine and Moroccan programmer with the name Merruktechnolog, allegedly opened more than 30,000 stolen iPhone gadgets within a few days of getting the stolen devices. To open those locked iPhones, the programmers utilized a Man-in-the-Middle assault and deceived the iPhone applications into joining with their server taking on the appearance of a real Apple server that is utilized to initiate Apple gadgets. When joined with the programmers' server, it will educate the iPhone gadgets to open. This is the first run through when any programmer has figured out how to bargain the exceptionally secured Apple's iCloud administration. iCloud is a cloud storage/ computing administration given by the Apple Inc. to its clients since October 2011 with more than 320 million clients over the world. The administration permits clients to store and move down information, for example, music, photographs, applications, reports, bookmarks, updates, reinforcements, notes, iBooks, and contacts, and gives a stage to Apple's email servers and datebooks (Khandelwal 2014).

In February 2005, Bank of America Corp. reported PC tapes containing MasterCard records of U.S. representatives and more than a million U.S. government representatives turned up missing, putting clients at very high danger of data fraud. In February 2005, a Georgia-based credit reporting organization had a break in its PC databases, rendering

about 145,000 individuals helpless against wholesale fraud. In June 2012, aggressors focused on Distributed Denial of Service (DDoS) mitigation benefit on CloudFlare by utilizing vulnerabilities as a part of AT&T's phone message administration for its portable clients. Likewise Google's record recuperation administration for its Gmail clients. There is additionally developing concerns in digital dangers to different systems, for example, power lattices and health awareness systems to use in terrorism, damage and data fighting. In the year 2009, Trojans were accounted for as up sixty percent of all malware. In the year 2011, this number has hopped up to seventy-three percent. The current rate shows that about three out of each four new malware strains made in 2011 were Trojans and demonstrates that it is the most popular weapon of choice for most digital offenders to lead system interruption and information theft. The arrangement of phishing endeavors implanted in eBay's sites comes months after more than 145 million usernames and key sets were found to have been stolen at some point around March 2014. Digital assaults are less expensive, more advantageous and they are known to be significantly less secure than direct physical assaults (Greatfire 2014).

1.3.3 An Emerging Type Of Security Compromise: Hacktivism

Hacktivism is a demonstration of political challenge, religious, or national discernment by non-legislative groups, inspired by the will to rectify what they see as the wrong laws and degenerate governments. This is particularly important to this paper because it is a type of activity that encompasses acts of terrorism/hacking. Hacktivism is such a threat because it does not only target small time pc users, it threatens to cripple governments and large businesses. These activities include the notorious groups like LulzSec and Anonymous groups. Hacktivists make a move against PC infrastructures typically utilizing the prominent, free apparatuses, some considered instruments "script kiddie", to dispatch a Denial of Service (DDoS) assaults, hack locales and open mode bending pages or sidetrack URL, or even release delicate information. A portion of the instruments equipped for computerized cyber attack. Usually, the goal of the struggle is to target oppressed nations such as Syria and Israel, on behalf of the oppressed people stepping up. In this case, the moral piracy seeks to improve the quality of life and the world. Although

hacktivists attacks are announced in advance, and the resulting success is not certain. The operations named #OpIsrael and #OpUSA (hashtag for "Operation Israel" to challenge unfairness to Palestinians by the Israeli government and hashtag "Operation USA" to dissent American outside approach) had low effect. Here and there delicate data can be spilled. Notwithstanding, DDoS assaults experienced by US banks in late 2012 and mid 2013 chopped down accessible transfer speed and had an in number effect. The point of the operations named #OpInnocence and # OpPedoHunt to stop the misuse of kids, while #OpGTMO was against the confinement camp at Guantanamo Bay. Interestingly, programmers got access to the Twitter record of The Associated Press for distribution of false data from the blasts in the White House. This trick plunged the United States stock market (Fernandes, Soares, Gomes, Freire, and Inacio 2014).

1.3.4 Five Reasons Why We Cannot Be Fully Cyber Secure

This thesis has talked about how the growing rate of cyber connectivity in the world makes it very vulnerable and susceptible to hacking activities. There are five main reasons why it is almost an impossibility for computer systems to remain cyber secure (Kessel, Allan 2014). These reasons are:

1. **Change:** In this post-financial emergency world, organizations need to move quickly. New items are being produced, mergers, buy-outs/take overs, market extension, and presentations of new innovation are all on the ascent: these progressions constantly have a confusing effect on the quality of an association's cyber security.
2. **Mobility:** Mobile computing brought about the smearing of organizational limits, with IT getting closer to the client and further from the association. The utilization of web, cell phones and tablets (in mix with bring-your-own-gadget) has made associations' information to be open all over the place.
3. **Ecosystem:** We live and work in a biological system of digitally associated elements, individuals and information, expanding the probability of the introduction of cybercrime in both the work and home environment.

4. **Cloud:** Cloud-based administrations, and outsider information management and storage, open up new channels of danger that did not initially exist.
5. **Infrastructure:** Closed operational technology systems are currently being given IP addresses. This has pushed cyber crime to advance out of the back-office frameworks and into critical infrastructures, for example, power generation, transportation frameworks, and also other computerized systems.

1.3.5 What Can We Do About Our Information Security?

The only possible way to completely secure a network/computer is by cutting off all access to the outside world, which is virtually impossible since the world has turned into a giant global village comprising of interconnected networks. Although it is impossible to be completely outside connection free, there are number of utilities and services which are freely or cheaply available that can aid in protecting corporations and social network users from being hacked. Several antivirus and security firms offer solutions for professional organizations in managing their networks and systems.

The easiest way to compromise a users network and access their data is through social media, by detecting and mitigating misbehaving social media accounts, users can be assured of a certain level of security when online.

One way of ensuring our security is through intrusion prevention. Intrusion prevention is the procedure of applying intrusion detection methodologies in an attempt to stop conceivable occurrences, intrusion prevention systems (IPSs) concentrate basically on distinguishing conceivable episodes, logging data about them, endeavoring to stop them, and then report them to security heads. Although firewalls are amazing at preventing intrusions to networks, with everyday evolving technologies, corporations and individual users need to be aware of emerging technologies to be able to keep up with the threats they pose to their security. By constantly auditing defense systems to ensure that a network's defensive armor can meet the latest threat. A dynamic and effective policy of constantly monitoring for suspicious activities is needed so that, when discovered, can be these suspicious activities can be quickly dealt with so that nothing slips past without consent.

One has to verify that their perimeter guards are as solid as they can be, and that implies staying aware of the quickly developing dangers around them. The times of depending singularly on a firewall that essentially does firewall duties are gone; today's saltines have made sense of how to sidestep the firewall by abusing shortcomings in applications themselves. Essentially being receptive to hits and interruptions isn't a decent alternative either; that is similar to remaining there holding up for somebody to hit you before choosing what to do as opposed to seeing the approaching punch and moving out of its way or blocking it. One has to be adaptable in their way to the most up to date innovations, continually reviewing your resistances to guarantee that your system's protective protection can meet the most recent risk. One needs to have an exceptionally changing and successful strategy of always observing for suspicious exercises that, when found, can be rapidly managed so somebody doesn't slip something past without them perceiving it. When that happens, it is past the point of no return.

A pivotal element for system chairmen is the need to instruct their clients. Regardless of how great a vocation they've done at taking care of their network security methods and frameworks, despite everything, they need to manage the weakest connection in their firm covering their clients. It doesn't benefit anyone to have impenetrable techniques set up in the event that they're so hard to deal with that clients work around them to maintain a strategic distance from the trouble, or on the off chance that they're so inexactly designed that a coolly surfing client who visits a tainted site will pass that disease along to your net-work. The level of trouble in securing ones system increments drastically as the quantity of clients goes up. User education gets to be especially essential where portable processing is concerned. Losing a gadget, utilizing it as a part of a spot (or way) in which prying eyes can see passwords or information, awareness to hacking devices particularly intended to sniff remote signs for information, and signing on to unsecured systems are all potential issue regions with which clients need to be well known (Vacca 2012).

Despite the fact that cybercrime and hacking have been around for more than 30 years, research in the area has been meager .It is found that 60 percent of the participants of the survey carried out by (Chantel 1996) confessed to taking part in criminal PC exercises, which shows the degree of this criminal conduct and why the world needs to worry more

about tackling it. The pervasiveness may be expected to some degree to the interesting profound quality encompassing this sort of criminal movement. The moral limits of innovation appear to be at chances with moral guidelines found in the genuine physical world. Numerous individuals feel that on the grounds that they are not managing substantial things – virtual documents rather than genuine property – the moral contemplations identifying with individual property and protection in the "genuine" world don't have any significant bearing in the "digital" world. This adaptable profound quality permits individuals to participate in practices in the "digital" world that they likely would maintain a strategic distance from in this present reality (Chantel 1996). Morals, or an obvious absence of them, have gotten to be such a worry, to the point that there have been a few warm level headed discussions encompassing this topic in the Information Technology area. Criminal conduct is kept up within a complicated timetable of fortification and discipline for the duration of the life of the individual. Considering PCs are the superhighways and hacking is a criminal action that depends on the reliance of PCs and Internet, there is motivation to accept that the programmer will be around for very much a while, so aggressive big/small firms and e-businesses need to ready themselves and protect themselves against illegal intrusions (Smith, Rupp 1993).

For corporations, making users aware of threats is one of the most useful solutions to avoid a crisis. Social network users need to be educated on the danger of following malicious accounts with bizarre activities, or opening up suspicious links from user accounts which are possibly embedded with viruses. For attacks attempts to be successful and compromise data integrity or confidentiality of information, the attacker has a to access first computer system secretly, intrude legitimate nodes, or access a power network in some way of authentication. Therefore, measure to protect against attacks that target the confidentiality of information can occur for the following perspectives (Wang, 2010).

1. Authentication Protocol Design
2. Intrusion Detection
3. Firewall Gateway Design

Subsequently, associations need to adapt to an endless cycle of new dangers and difficulties obliging the selection of an endless cycle of change and re-assessment of the changing cyber security capacities. Associations need to create a system that empowers

them to deal with this cycle in a proficient and compelling way so that they have an advantage from grasping new/diverse security opportunities, which, thusly, empower the business and save expenses (Kessel, Allan 2014)

Additionally, security experts can set up bogus networks or user accounts to bait hackers into making an attempt on them. Experts can then notice the activities of hackers and gain valuable data on the methods, tools, and any new malware they might be using. Table 1.1 gives an example of common cyber attacks and their counter measures (Jang-Jaccard, Nepal 2012).

Table 1.1: Common Cyber Attacks and There Counter Measures

	Hardware	**Software**	**Network**
Common Attacks	-Hardware Trojans -Illegal Clones -Side Channel Attacks	-Programming bugs -Design Bugs -Deployment Errors	-Networking Protocol Attacks -Network monitoring and sniffing
Examples of Counter Measures	-Tamper Resistant Hardware -Trusted Computing Base -Hardware Watermarking	-Secure Coding Practice -Code obfuscation -Secure Design and Deployment -Formal Methods	-Firewall -Intrusion Prevention and Detection -Virtual Private Network -Encryption

Source: Jang-Jaccard, Nepal 2012.

1.3.5.1 CSI report of financial related misfortunes due to cybercrime

To shed some more light on to the severity of cyber security mishaps, this paper investigates the 2008 CSI Survey. According to the survey, the graph of normal financial related misfortunes because of cybercrime has looked like nothing more than an illustrative line nearing an even asymptote. There was a time, a while ago in which reported misfortunes dropped fundamentally, followed by a hop a year ago, dropping again not long from now. The thought of generally low misfortunes isn't a thought that plays well in specific fragments of the PC security group. This is especially valid among specialists who are effectively occupied with managing the more terrific criminal acts that unavoidably happen every year. It is imperative to perceive that while there are a modest bunch of marvelous unlawful acts in a year, there is a large number of big businesses arrangements that don't stand out as truly newsworthy. We should besides draw a refinement between creating dangers and real effective assaults. There is, foundation for great concern with respect to the sorts of assaults that get to be conceivable as we move to a more administration situated Web, however these are not dangers hat have seen far reaching utilization yet, at any rate not among those reacting to the survey (Richardson 2008).

1.3.6 Understanding Hackers

When discussing IS, one must also talk about the people whom are responsible for finding and exploiting the vulnerabilities of a system or network. A hacker is somebody who ignores tried and proven ways of thinking and does something else, a person who think outside of the box, Somebody who sees an arrangement of rules and miracles and then wonders what happens in the event that you don't follow them. A hacker explores different avenues regarding the limits of frameworks for erudite curiosity. A lot of studies about hackers have concentrated on individual and social behavioral attributes taking into account identity and inspiration profiling. Analyzing the mental methods of hackers empowers researchers to have knowledge into their decision making and learning.

Social cognitive Theory (SCT) refers to a mental model of conduct that rose basically from the studies of Albert Bandura. It was made with an emphasis on the securing of

social practices, SCT keeps on underscoring that learning occurs in a social setting and that quite a bit of what is discovered is increased through perception. SCT has been connected to various regions of human working as profession decision, hierarchical conduct, games, and mental and physical wellbeing. SCT incorporates an extensive number of discrete thoughts, ideas, and sub-forms into a general system for the comprehension of human workings.

Taking this cognitive research methodology offers a chance to see how the hackers' personality interprets reality, how hackers decide, and how their thoughts coincide with language. To understand the personal and social cognition among hackers, how they build and keep mental models. Timothy C. Summers carried out a research. He found that hacking as a cognitive activity, calls for an excellent specialized thinking capacities and mental models can be considered as a hackers inward representation of the parts and working guidelines of software and equipment frameworks that empower them to investigate and distinguish its vulnerabilities. This gives bits of knowledge into seeing how a system may work [or malfunction], how different parts of that system communicate, and how those associations produce particular activities. Accordingly, the specialized and thinking capacities needed for PC programming are needed for participating in hacking. Likewise, mental models used in hacking incorporate, yet are not restricted to, techniques of writing code, investigating different systems and project perception related tasks. These mental models help hackers portray, clarify, and anticipate a systems characteristics and practices. In particular, they allow hackers to depict the system's purpose and structure, clarify watched states and systems usefulness, and foresee future system states (Summers 2013).

During the interviews carried out on hackers in the research by (Summers 2013), the participants of the research survey were asked different questions with respect to their experience, areas of mastery, their hacking practices, and any hacking issues or circumstances that they could remember and portray. Their cognitive processes were reviewed and problems they encountered. Their sentiments about hacking exercises were examined, connections and correspondence with different hackers, suppositions on utilizing drawings, outlines, pictures, and different representations amid hacking.

Five main patterns were discovered amongst hackers: Cognitive patterns, predictive patterns, learning patterns, engaged patterns and comprehensive patterns.

Qualified hackers perform subtly within poorly characterized environments. Keeping in mind the end goal, which is to successfully handle the danger, vulnerability, unclearness, and bedlam connected with working inside such an environment, they needed to influence information, inventiveness, interest, ability, and interpretive plans from different specialized and critical thinking disciplines. Hackers acknowledge vagueness as an after effect of the quickened innovative changes that happen around them. Hackers needed to utilize intelligent deduction and reflection to apply their own mental rationale and comprehension to manufacture a mental representation of the system or a physical topology of the system to help them see the structure and physical association of it. One hundred percent of respondents of the survey reported individual reflection as a method for building and keeping up hackers' mental models. Strategizing and decision-making are one of the main aspects of being a hacker. That is the way they are able to discover such novel and imaginative approaches to break into and secure systems in such complex situations and circumstances. Notwithstanding, no hacker does this in a vacuum. They utilize social communication and trades through talk to figure out how to distinguish the most likely results, select the most invaluable techniques and settle on the best choices. Hackers additionally utilized gathering discourses to connect with as a part of social cognition and to together investigate the issue or target a system.

Eighty-three percent of respondents in the survey utilize social talk as an instrument of information exchange instrumental for comprehension nature and making significance of the related instability. Although qualified hackers use patterning all through their work, a standout amongst the most fascinating uses is in their capacity to perform groundbreaking activities. Talented hackers utilize patterning to support them as a part of envisioning future occasions and making techniques for tending to those occasions before they happened. Execution of these activities depends intensely on a mental rationale, both collective and individual, it also depends on specialized skill, imagination and interest, and considerable mental ability to rapidly manufacture and control mental models immersed with many-sided complexities (Summers 2013).

It is understood that mental models and cognitive systems play a major role in the activity of hacking. As the world gets to be more dependent on computerized innovations, as countries and organizations coordinate hacking into their antagonistic tool compartments,

a cognitive structure of hackers can give generous understanding into seeing how to secure ourselves, advance, and build up the up and coming era of hackers.

1.4 LITERATURE REVIEW

Taking into account the study of Self-Efficacy, this thesis analysis the security perceptions in the shaping of human behavior as its core literature review. It will take this literature review into account when discussing the findings of this thesis.

People with high Self Efficacy in Information Security utilized more security software and highlights. The appropriation rate of the real security applications, and of extra security devices, was higher with high Self-Efficacy in Information Security people. Moreover, this gathering of clients connected security overhauls/fixes more frequently than people with low Self Efficacy in Information Security (SEIS). SEIS impacted the utilization of security software as well as the security care conduct identified with PC/Internet use. People with high SEIS made backup duplicates of imperative documents all the more much of the time, used solid and various passwords for diverse online accounts, checked whether the website scrambles exchanged information when sending their own data, and did not impart their PCs to other individuals. Moreover, clients with high SEIS exhibited their proposition to proceed with and fortify these security endeavors. Steady with social cognitive viewpoint on processing conduct, these outcomes recommend that self-efficacy is a critical develop in deciding people's information security hones. It is affirmed that self-efficacy in data security is an important discourse in understanding security practice behavior. From a handy point of view, the discoveries propose that IS experts need to be mindful of the role of users' conviction on their efficacy in the data security space on security practice conduct. They have to outline training projects that all the more successfully encourage this efficacy conviction. It is proposed that a preparation program that upgrades SEIS can bring about a larger amount of security practice behavior regarding both utilizing innovation and security aware care behavior. In this manner, essentially posting what not to do and punishments connected with a wrong doing in the users' information security arrangement alone will have a constrained effect on viable usage of efforts to establish safety. The consequences of this

study likewise show that the general controllability impression of IS dangers is decidedly connected with SEIS. Current security mindfulness training stresses the powerlessness identified with the different IS dangers and what ought not be carried out to diminish such weakness. Given the impact of general controllability discernment to SEIS, awareness training ought to likewise convey the presence of means and strategies to control IS dangers (Rhee, Kim, Ryu 2009). The literature review covered in this section of the thesis explores the existing method of determining IS security awareness. It explores the already existing theories of measuring awareness, these theories will be used in the survey carried out in this paper to understand how students think and how their actions affect there is awareness level although it focuses mainly on the security perception in the shaping of planned behavior using self-efficacy and the theory of planned behavior.

1.4.1 Security Perception In The Shaping Of Human Behavior

The impact of Computer Self Efficacy on PC use and selection has been exhibited in earlier studies. Research on Computer Self Efficacy demonstrated a noteworthy positive relationship between clients' trust in their figuring abilities and utilization of data systems. Example, Internet self-efficacy has been indicated to be a positive affecting variable for Internet utilization and utilization of an e-administration. Social cognitive hypothesis likewise underlines the part of self-efficacy on conduct control over conceivably undermining occasions. Individuals with a solid feeling of self-efficacy are likely centering their consideration on investigating and defining answers for issues. Those with low self-efficacy have a tendency to take part in less adapting efforts. Individuals keep their behavior in accordance with their own models through self-evaluative response (Bandura 1986). Any errors between conduct and individual models produce self-reactive impacts, which serve as helpers and aides for activity intended to accomplish desired results (Rheea, Kimb, Ryuc 2009).

1.4.1.1 Online security

As Information Security is only applicable in an online environment, this section takes a look at IS providers, that is, online security sites and how they shape the behaviors of clients that visit the sites in search of better online security measures. Generally speaking, existing online security sites have a tendency to stretch the apparent seriousness of and defenselessness to online safety dangers, energize the utilization of preventive measures, and highlight how viable the measures are in tending to the potential dangers. In this way, it may be said that "scare tactics" are the transcendent correspondence system found at online safety sites today.

Engages to moral standards were very visible in the research carried out by (LaRose, Rifon, Liu, Lee 2015). During their security websites assessment, in the domain of online security, differing perspectives have risen on the best way to secure Internet clients. Some vibe that Internet administration suppliers ought to set up firewalls and naturally redesign protection software, others would put the weight on operating systems and web designers, while others advocate more noteworthy government mediation. To better advance a feeling of moral obligation, online security mediations could bring up the characteristic restrictions of depending on outsiders. For instance, the consistent event of new dangers, the slack times needed to actualize viable technical solutions, and the developing expense of those answers for the purchaser may be underlined. Examples of overcoming adversity of courageous Internet clients who distinguished and neutralized perils that accessible software securities neglected to discover may likewise further the objective of moral obligation. Generally, the present sites gave careful consideration to how the Internet clients can get to be sure about establishing their own preventive conduct. The few that did have a self-efficacy concentrate just offered shallow admonishments about the simplicity of establishing protections, some of which (e.g., the simplicity of introducing firewalls) may appear to be overstated to numerous online clients.

Seen self-efficacy toward oneself is a key variable on the grounds that it works on inspiration and action both specifically and through its effect on alternate determinants (Bandura, 1998).

What online security sites are knowledgeable in are "do nots." for instance, "don't open an email attachment from an unknown individual." In hypothetical terms, such

explanations are calls to action. They can encourage the preparation to act. Furthermore, they can enhance self-efficacy. The more information clients have of perils to stay away from, the more sure they are in their capacity to secure themselves. Verifiably, they are likewise explanations about reaction adequacy, since online security campaigns would clearly not prescribe activities that were not accepted to be viable (LaRose, Rifon, Liu, Lee 2015).

Self-efficacy is defined according to the psychologist, Albert Bandura as the confidence in an individual's abilities to create and carry out the approaches needed to oversee planned situations. Self-efficacy toward oneself is an individual's trust in his or her ability to succeed in a particular situation. Bandura delineated these feelings as determinants of how people think, bear on, and feel emotion (Bandura, 1994). People who effectively look for information about security online are already concerned about online safety, think they are powerless against assault, and without a doubt might regularly visit these sites in light of an assault. In the meantime, they are unlikely to have elevated amounts of PC security knowledge and without a doubt the sites are not addressed to system security experts. So, the accentuation on scare tactics could be counterproductive, since the guests are prone to have low self-efficacy and therefore may have their apprehension further excited as opposed to enact security. In the present exploration, techniques that enhance self-efficacy were discovered to be uncommon as well as shallow, attempting to convince guests that to a degree, overwhelming assignments were truly simple to perform. Methodologies that calm tension and that create enactive dominance (Bandura, 1997) by controlling clients to finish logically more troublesome self-protective tasks may be more viable (LaRose, Rifon, Liu, Lee. 2015).

2. MATERIALS AND METHODS

2.1 RESEARCH HYPOTHESES

This thesis creates a research model which investigates the relationship between gender, age, university location and department as determinant factors of the awareness level of students i.e. if their knowledge of information security awareness is based on any of them above-mentioned variables, as seen in figure 2.1. The third section of this thesis will prove, based on the statistical analysis that will be carried out, the hypotheses pointed out. Each hypothesis holds one variable, which will be weighted against the students' answers to a certain question that will be used to judge their perception of their individual security awareness levels.

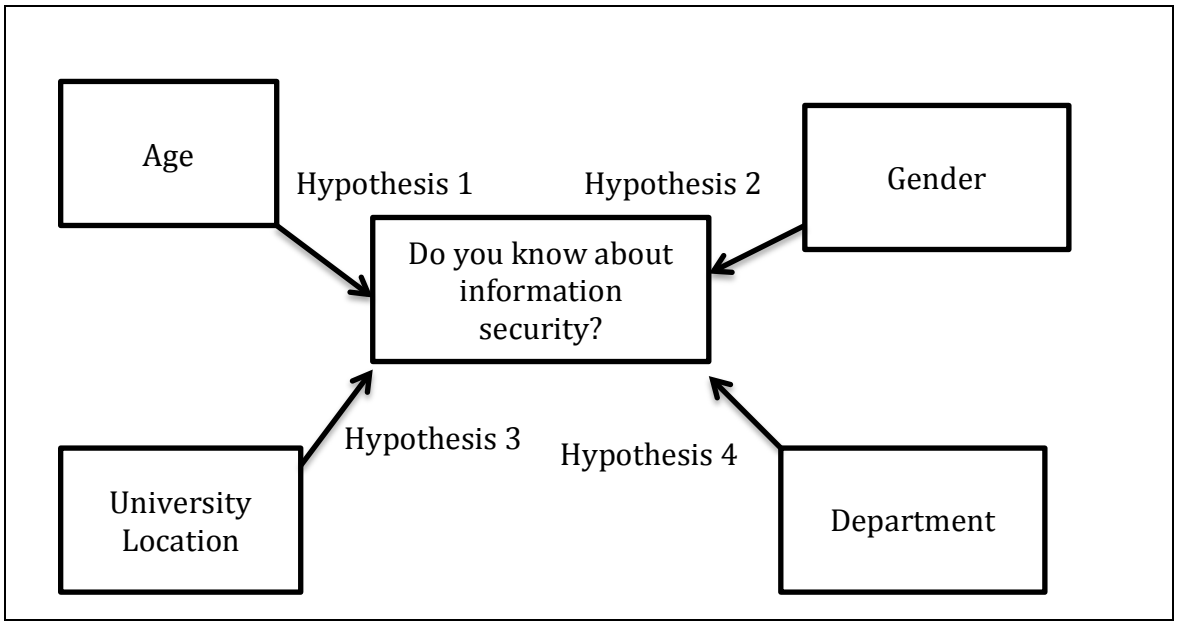
Hypothesis 1: Age is a determinant factor in the information security awareness level of students.

Hypothesis 2: Gender is a determinant factor in the information security awareness level of students.

Hypothesis 3: Location of the university is a determinant factor in the information security awareness level of students. Hypotheses 3 will weigh the locations of all students against how they perceive their knowledge of information security, this will be used to find out if the individual locations of the universities of all students have to do with their answers meaning some countries prioritize IS education more than others.

Hypotheses 4: Department of students is a determinant factor in the information security awareness level of students.

Figure 2.1 Research Model



Source: Aliyu M.A, Istanbul 2015.

2.2 SURVEY

Data Analysis is the procedure of checking, fixing and modeling facts with the aim of bringing out relevant information, coming up with suppositions and support the decisions made from the information gotten from the data analyzed. For the purpose of this thesis, a survey will be carried out to evaluate cyber security threats. The survey targets University students from different departments across different countries and age groups. The data from the questionnaire answered by the students will be used to determine how aware students are of Information security threats. Location, age and department are all factors that will determine the awareness level of the students (Security Awareness Survey, 2012).

2.2.1 Student Security Awareness

Most Universities teach Information Security in the final year or at the master's level and this usually applies to students at the Engineering or Computer Sciences departments.

This is not efficient because students have already learned how to use computers earlier on in their levels without knowing how to protect themselves/their devices and data from security breeches. Contrary to popular belief, not only big companies are at a risk of malicious activities aimed at exploiting their data and security, small business and also students run a major risk of security breeches.

It is clear that students need to be educated about security issues early, the earlier they are aware of Information Security vulnerabilities, the safer they will be in the future as they will be able to pay more attention to security matters and also avoid engaging in illegal behavior. The more knowledge of Information Security that parents and teachers have, the more students and youngsters will be taught and prepared for any security occurrences.

2.3 CONDUCTING SECURITY AWERENESS SURVEY TO STUDENTS

Information Security awareness of students is measured by Security Awareness survey. This survey will be used to ask students how they would respond to specific security related questions and situations. The results of this survey can be used to assess how vulnerable students are in terms of Information Security and what needs to be improved this done by computation of a risk score.

There were two steps that were taken in determining the outcome of this survey. A pre-test Analysis was carried out which involved 43 students while the post-test analysis performed with 103 students. This was necessary in order to determine the optimum result from this survey.

2.3.1 Using This Survey to Determine Risk/Vulnerability Score for Security Awareness

There are 21 questions in the Survey (look Appendix I for survey questions). Each of these questions has a risk value, which indicates strong awareness and good security practice or weak awareness and bad security practice. The questions have been assigned a risk value between 1 and 5 based on the Likert scale. At the end of the survey, the results

can be used to calculate the overall risk level and vulnerability score of students (Security Awareness Survey, 2012).

1. Each questions' risk value will be multiplied by the number of times it was chosen by subjects.
2. All response totals will be added together to get a survey cumulative response total.
3. The surveys cumulative response total will be divided by the number of survey takers to calculate the students risk score.
4. By using the students' risks scores for the students general risk rating will determine the risk level of each student as given in Table 2.1.

Table 2.1: Risk Analysis

Risk Level	Description
Low (10-25)	Students are aware of Security threats and how to mitigate them. They have knowledge of security standards and policies and also apply them.
Below Average (25-50)	Students are aware of security threats, have knowledge of security policies and standards but do not apply them.
Average (51-75)	Students are aware of security threats; they have no knowledge of security standards and policies but also do not take any measures against them or take part in activities that put them at risk.
High (76-100)	Students are not aware of security threats and policies. The take part in activities that can easily be used to exploit them.

Source: Security Awareness Survey, 2012.

(Survey minimum risk score= 25; Survey maximum risk score=100)

2.3.2 Survey Deployment

1. Students from different Universities and departments will be asked to take part in this survey.
2. Students will be evaluated based on what they have answered from the survey.

3. Survey will be carried out voluntarily.
4. Survey will be uploaded onto a Survey monkey file for a wider reach of students.
5. Results will be discussed at the end of the Survey after online survey has being closed.
6. Post-test was deployed 3 months after deployment of pre-test.
7. Both the pre-test and post-test surveys were deployed in the same manner.

2.4. SECURITY AWERENESS SURVEY PRE-TEST PHASE

The 43 students from different departments from different Universities across the world took part in this survey. The survey was posted on Google drive for duration of one week and students were asked to volunteer. Each student answered all 21 questions of the survey. They were students from departments such as:

I. Electrical Electronics Engineering
II. Business Administration
III. Cinema and Television
IV. Political Sciences
V. Economics and Administration
VI. Aviation Management
VII. Psychology
VIII. MBBS
IX. Nanotechnology and Biochemistry
X. Finance

Each questions risk value was multiplied by the number of times it was chosen by survey takers.

Question 1, 20 and 21 had no risk value, starting from Question 2-18; the response total of each question was gotten and tallied in table 2.2.

Table 2.2: Pre-test Risk Value Score

Question Number	Risk Value Score
2	220
3	150
4	143
5	120
6	118
7	130
8	151
9	124
10	117
11	163
12	103
13	110
14	154
15	98
16	92
17	120
18	103
Cumulative Total	2216

Source: Aliyu M.A, Istanbul 2015.

2.4.1 Statistical Analysis for the Pre-test of the survey

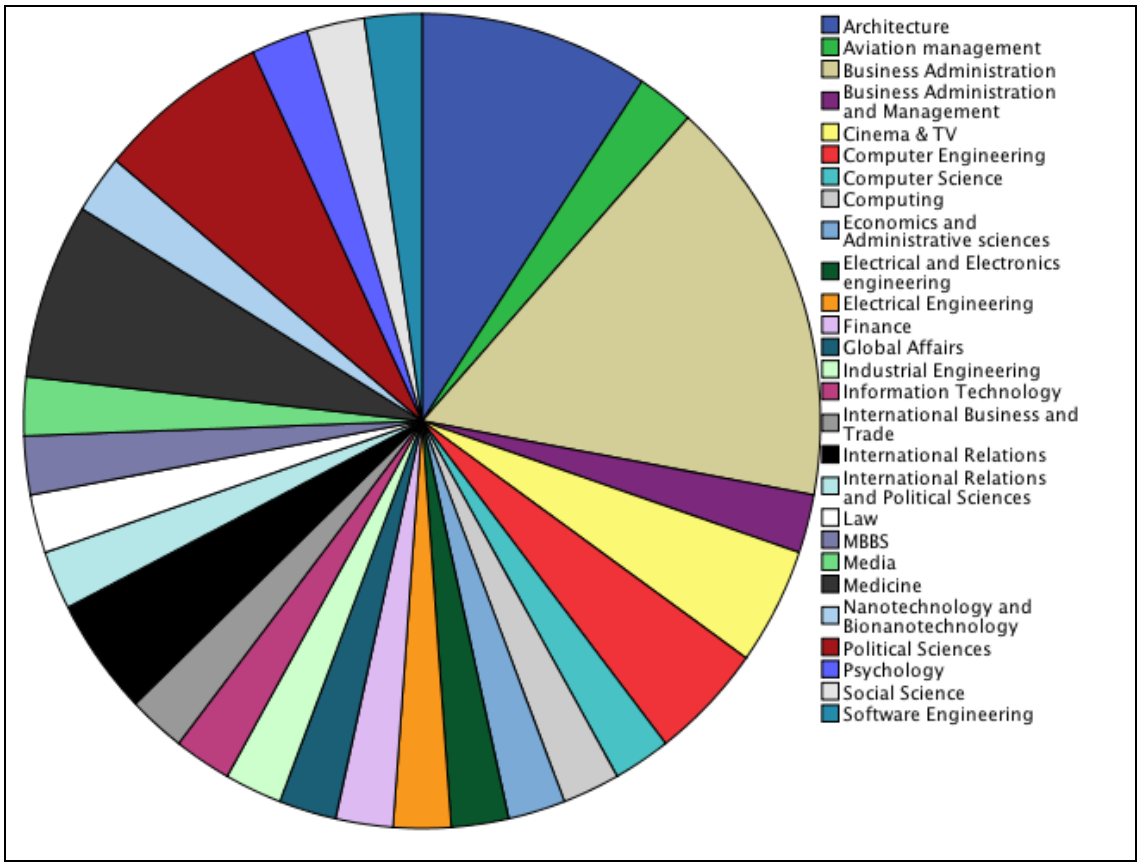
Statistical analysis carried out in this thesis was performed with IBMs SPSS software. The data gotten from the survey were downloaded into a csv file. The csv file was then uploaded to IBM SPSS Statistics software where data analysis was done. The statistical output data was downloaded and converted into a word file. Below are the results from the analysis, frequency tables, statistics and charts. These results will be used to prove the awareness levels of students and what factors affect their awareness levels.

2.4.1.1 Details for pre-test variables

Pie Charts depict the survey variables and the answers that the students chose. Each color depicts a variable in the survey. Below each chart is a tabular numerical representation of the depicted pie chart. The questions asked in the questionnaire (see Appendix I) will be referred to as variables during this analysis numbered Variable 1-21. A frequency and statistical analysis will be carried out on each variable in this section:

1. What is your department?
2. What is your age?
3. Where do you school (Location)?
4. What is you Gender?
5. If you delete a file from your computer or USB stick, that information can no longer be recovered.
6. My computer has no value to hackers, they will not target me.
7. Is anti-virus currently installed, updated and enabled on your computer?
8. Do you know what an email scam is and how to identify one?
9. Do you know what phishing attack is?
10. How careful are you when you open an attachment in email?
11. Has your computer configured to be automatically updated?
12. Is the firewall on your computer enabled?
13. How secure do you feel your computer is?
14. If you format a hard drive or erase the files on it all the information on it is permanently lost.
15. Does anyone have your computer password?
16. Do you know how to tell if your computer is hacked or infected?
17. Have you ever found a virus or Trojan on your computer?
18. Do you know who to contact in case you are hacked or if your computer is infected?
19. If your computer is hacked, can you do something about it?
20. Do you know about Information Security?
21. Do you own a personal computer?

Figure 2.2: What is your department?



Source: Aliyu M.A, Istanbul 2015.

Table 2.3 shows the numerical representation of the chart in figure 2.2. The students were spread randomly between 27 departments; some departments had multiple survey takers whom were students of that department while others had only one student. All 43 of the students whom took part in the survey belonged to one of the departments in the table 2.1. As seen in figure 2.2, the results of the survey carried out in this survey were based on the departments of the students. Figure 2.2 and table 2.3 depict each department and its frequency (How many students were from that department). Students from the departments Aviation management, Finance, Global Affairs, Industrial Engineering, Information Technology, International Business and Trade, International Relations and Political, Sciences, Law, MBBS, Economics and Administrative sciences, Computing, Computer Science, Business Administration and Management, Electrical and Electronics engineering, Electrical Engineering, Media, Nanotechnology and Bio nanotechnology, Psychology, Social Science, Software Engineering had a 2.33 percent

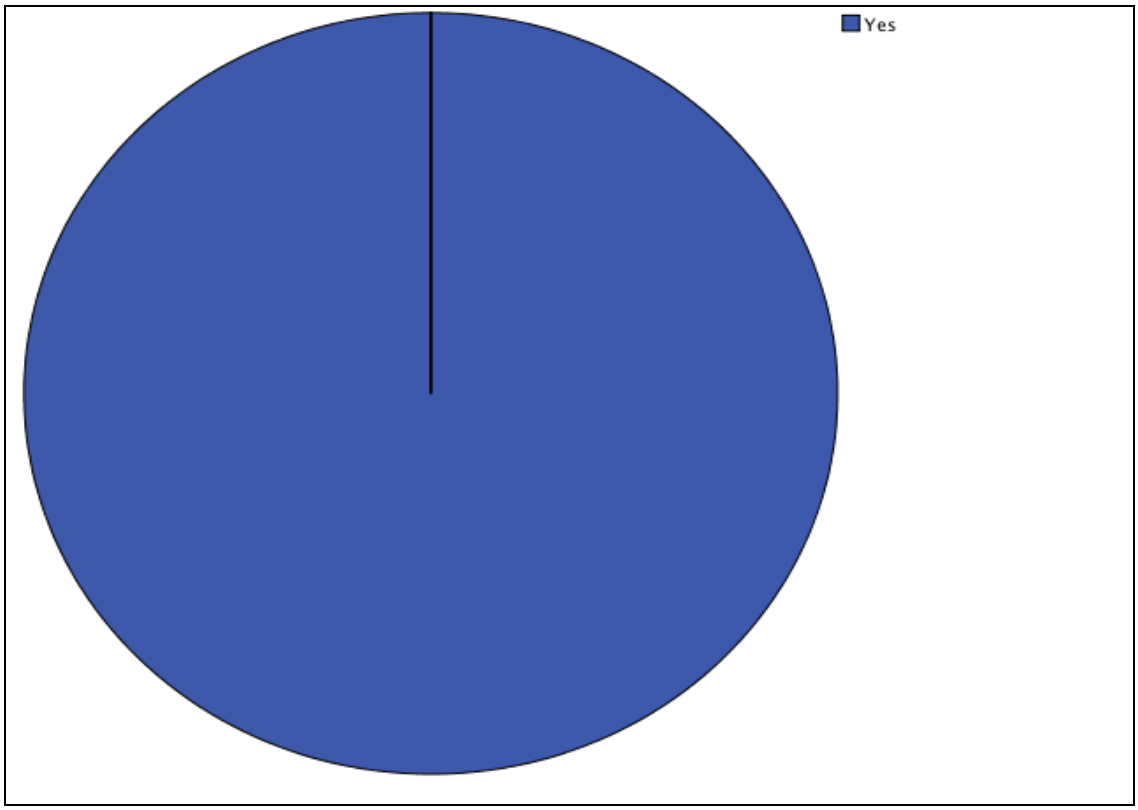
average frequency each (1 student each). 9.3 percent of the students were from the Architectures department (4 students). 16.28 percent were students of Business Administration. Students Cinema & TV (2 students each), Computer Engineering and International relations had a 4.65 percent each (2 students each). Students from the Medicine and Political Sciences departments had a 6.98 percent (3 students each).

Table 2.3: Variable 1 Chat Statistics

Architecture	4	Finance	1
Aviation management	1	Global Affairs	1
Business Administration	7	Industrial Engineering	1
Business Administration and Management	1	Information Technology	1
Cinema & TV	2	International Business and Trade	1
Computer Engineering	2	International Relations	2
Computer Science	1	International Relations and Political Sciences	1
Computing	1	Law	1
Economics and Administrative sciences	1	MBBS	1
Electrical and Electronics engineering	1	Media	1
Electrical Engineering	1	Medicine	3
		Nanotechnology and Bionanotechnology	1
		Political Sciences	3
		Psychology	1
		Social Science	1
		Software Engineering	1
		Total	43

Source: Aliyu M.A, Istanbul 2015.

Figure 2.3: Do you own a personal computer?



Source: Aliyu M.A, Istanbul 2015.

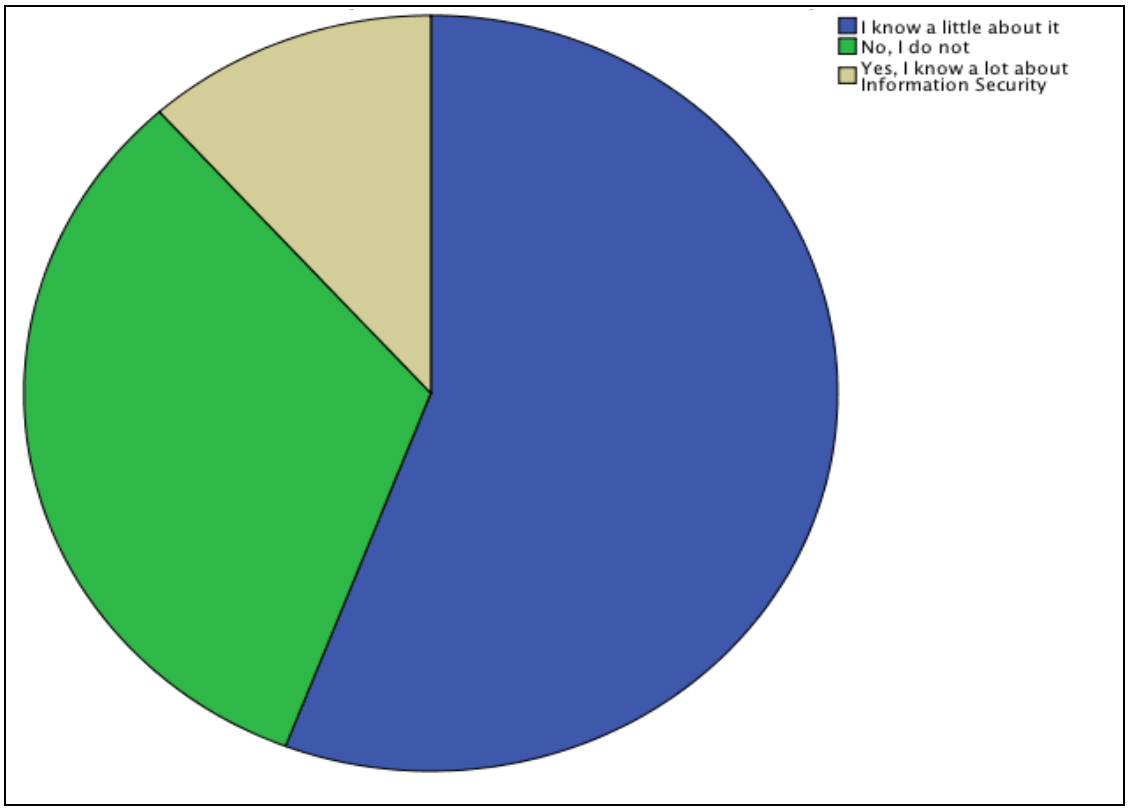
Table 2.4: Variable 2 Chat Statistics

Yes	43

Source: Aliyu M.A, Istanbul 2015.

Table 2.4, which is a numerical representation of figure 2.3, shows that all 43 students, a 100 percent, answered yes to the question in variable 2.

Figure 2.4: Do you know about Information Security?



Source: Aliyu M.A, Istanbul 2015.

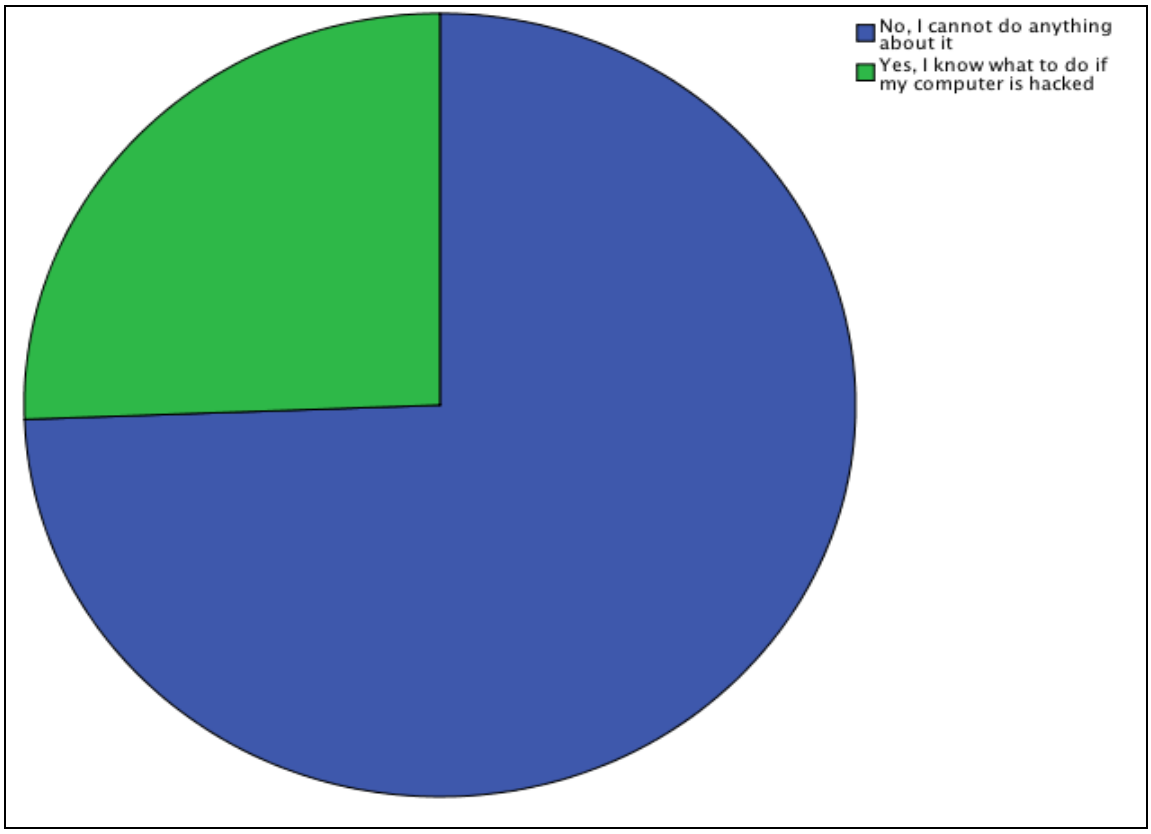
Table 2.5: Variable 3 Chat Statistics

I know a little about it	24
No, I do not	14
Yes, I know a lot about Information Security	5
Total	43

Source: Aliyu M.A, Istanbul 2015.

24 of the students which is 55.81 percent of response total of variable 3 answered, "I know a little about it" to the question in variable three, 14 of the students, 32.56 percent, answered "No, I do not know" and 5 of the students, 11.63 percent answered "Yes, I know a lot about Information Security" as seen in table 2.5 which is a numerical representation of figure 2.4.

Figure 2.5: If your computer is hacked can you do something about it?



Source: Aliyu M.A, Istanbul 2015.

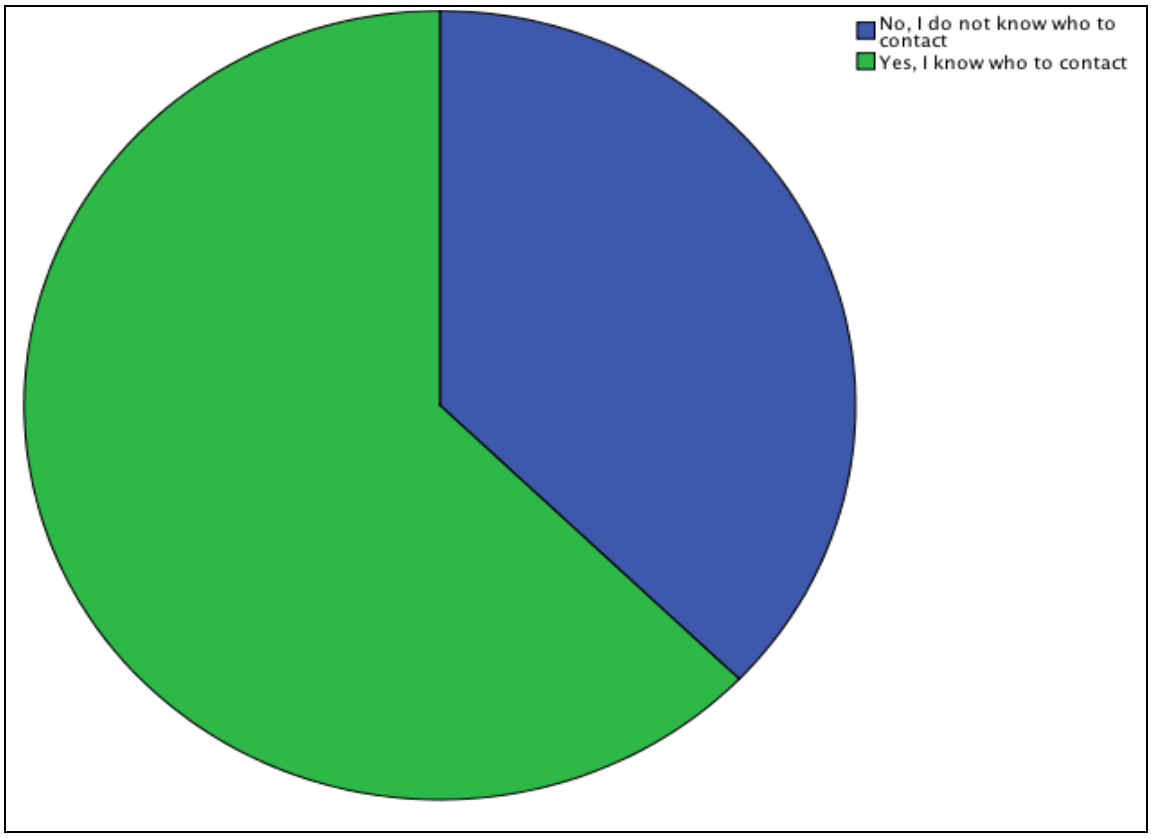
Table 2.6: Variable 4 Chat Statistics

No, I cannot do anything about it	32
Yes, I know what to do if my computer is hacked	11
Total	43

Source: Aliyu M.A, Istanbul 2015.

Figure 2.5 depicts the graphical representation of variable 4 and the responses of the students. Out of the 43 students of the survey, 32 of them, as seen in table 2.6 answered "No, I cannot do anything about it" which is a 74.42 percent of the response total of the variable 4. 25.58 percent answered, "Yes, I know what to do if my computer is hacked".

Figure 2.6: Do you know who to contact incase you are hacked or if your computer is infected?



Source: Aliyu M.A, Istanbul 2015.

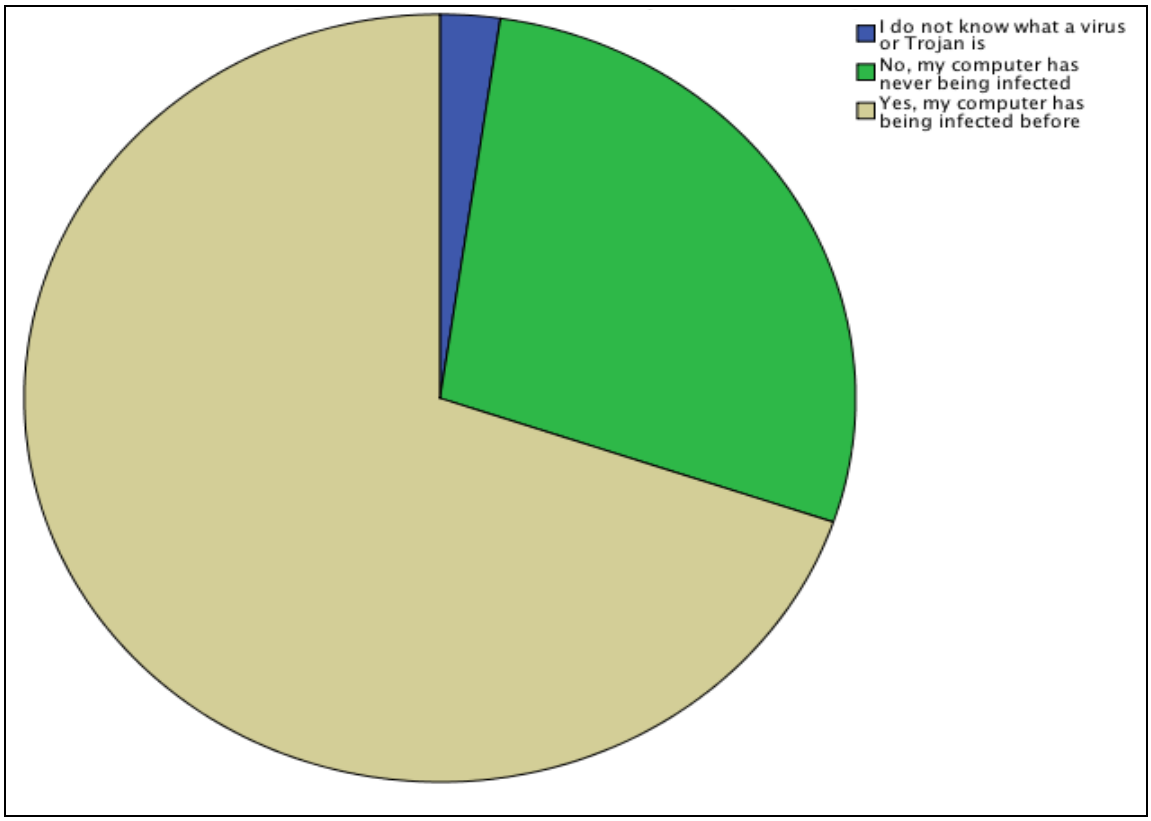
Table 2.7: Variable 5 Chat Statistics

No, I do not know who to contact	16
Yes, I know who to contact	27
Total	43

Source: Aliyu M.A, Istanbul 2015.

In figure 2.6, 37.21 percent of the students answered "No, I do not know who to contact" that is, 16 out of the 43 students as seen in table 2.7 while 62.79 percent of them answered "Yes, I know who to contact".

Figure 2.7: Have you ever found a virus or Trojan on your computer?



Source: Aliyu M.A, Istanbul 2015.

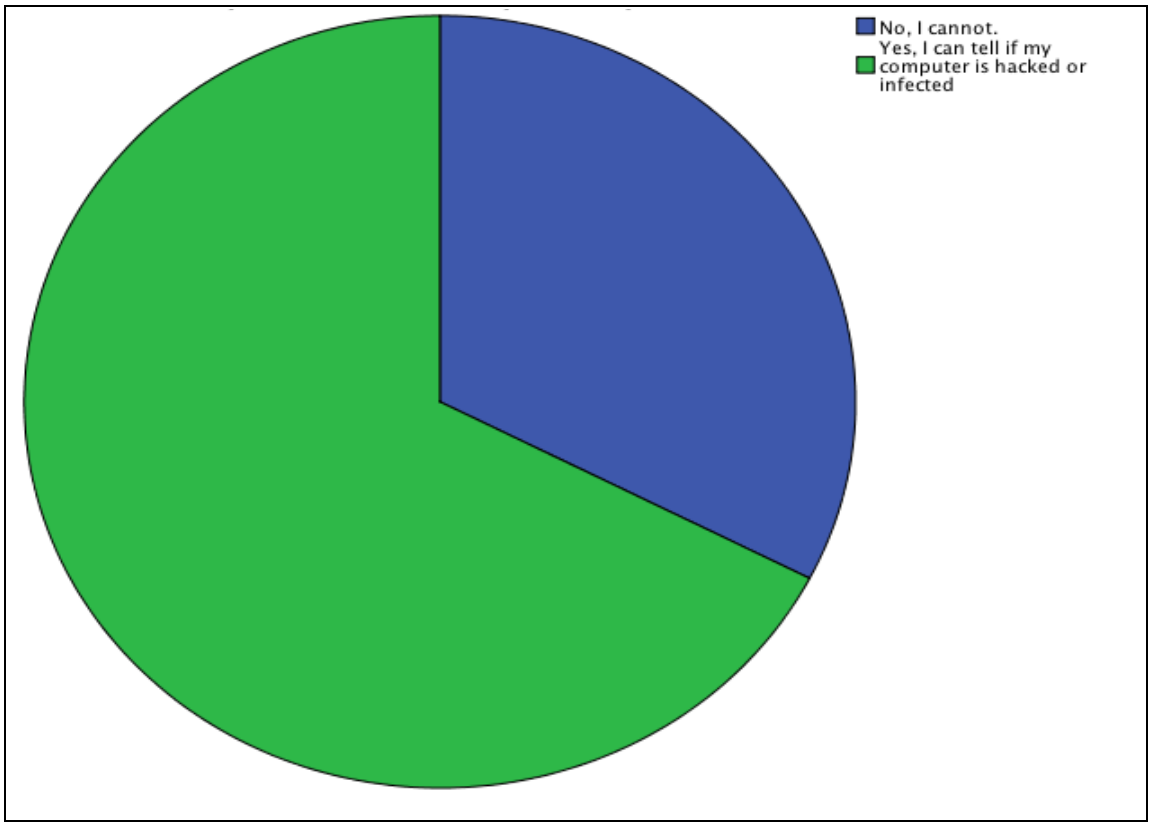
Table 2.8: Variable 6 Chat Statistics

I do not know what a virus or Trojan is	1
No, my computer has never being infected	12
Yes, my computer has being infected before	30
Total	43

Source: Aliyu M.A, Istanbul 2015.

Students were asked in figure 2.7 if they had ever found a virus or Trojan on their computers. 2.33 percent answered "I do not know what a virus or Trojan is" that is, just one student gave that response as seen in table 2.8, 27.91 percent (12 students as in table 2.6) answered "No, my computer has never being infected" and 69.77 percent (30 students) answered "Yes, my computer has being infected before".

Figure 2.8: Do you know how to tell if your computer is hacked or infected?



Source: Aliyu M.A, Istanbul 2015.

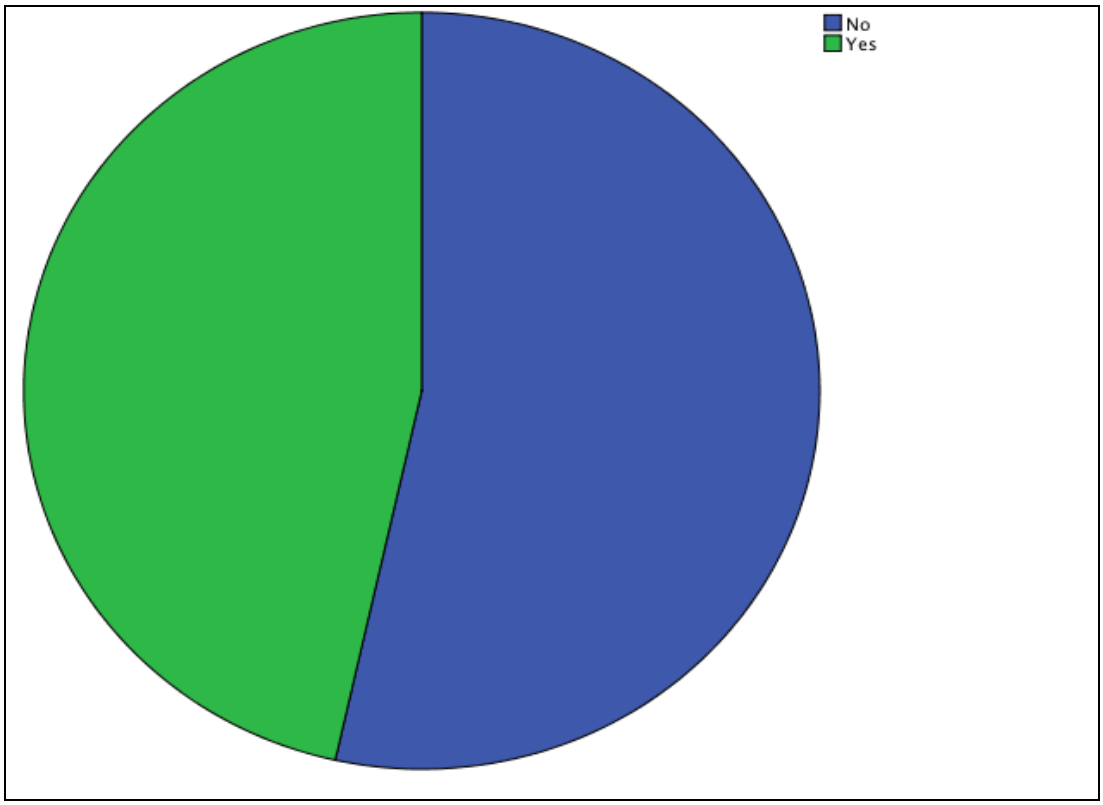
Table 2.9: Variable 7 Chat Statistics

No, I cannot.	14
Yes, I can tell if my computer is hacked or infected	29
Total	43

Source: Aliyu M.A, Istanbul 2015.

Table 2.9, which is a numerical representation of figure 2.8 shows that 14 students, which is 32.56 percent of the students answered, “No, I cannot” when asked if they could tell if their computer was hacked or infected while 29 students, 67.44 percent answered, “Yes, I can tell if my computer is hacked or infected”.

Figure 2.9: Does anyone have your computer password?



Source: Aliyu M.A, Istanbul 2015.

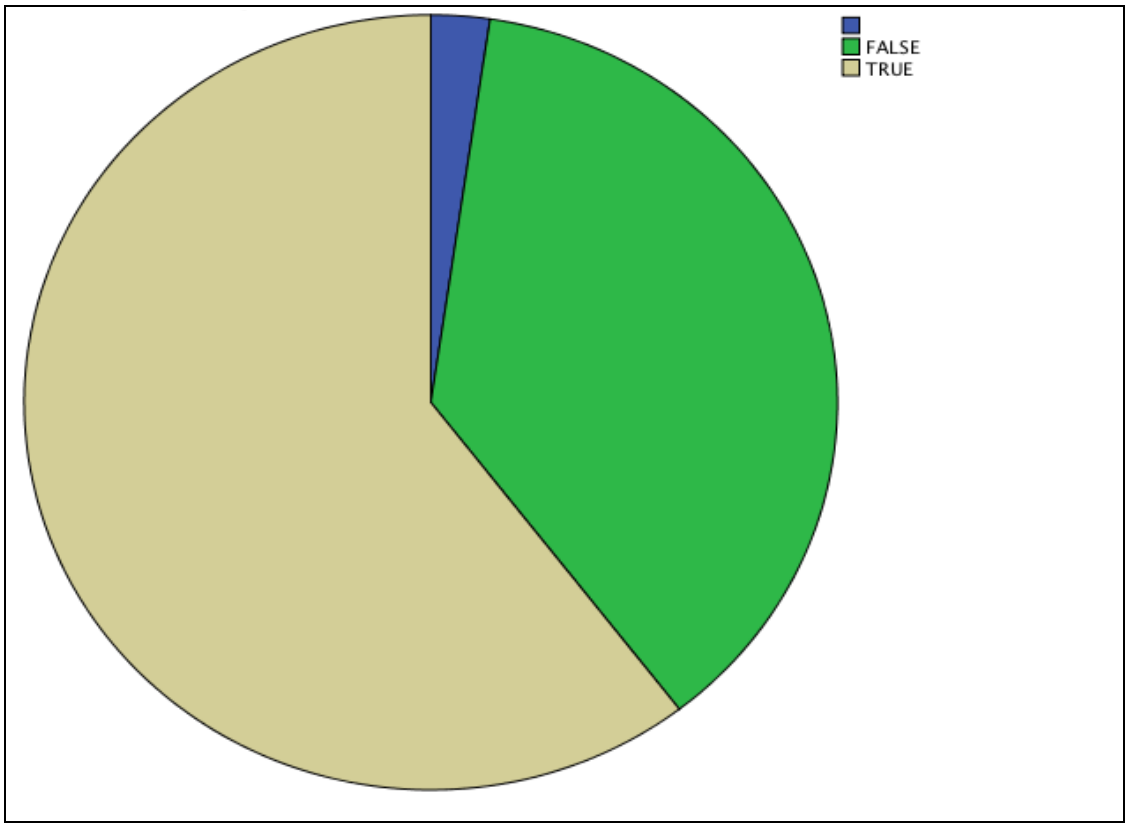
Table 2.10: Variable 8 Chat Statistics

No	23
Yes	20
Total	43

Source: Aliyu M.A, Istanbul 2015.

Table 2.10 gives the numerical representation of figure 2.9, 53.49 percent, which is 23 of students answered "No" to the question; does anyone have your computer password? while 20 students, which is 46.51 percent answered, "Yes".

Figure 2.10: If you format a hard drive or erase the files on it all the information is lost.



Source: Aliyu M.A, Istanbul 2015.

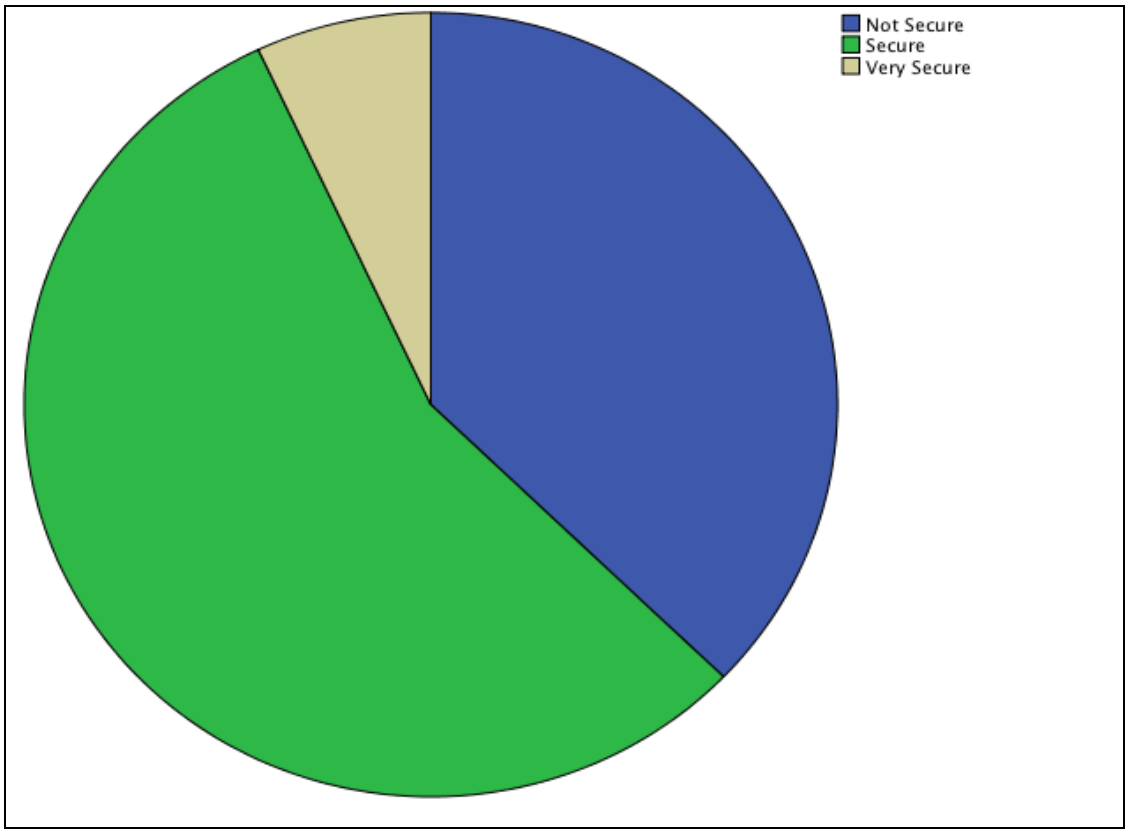
Table 2.11: Variable 9 Chat Statistics

None Valid	1
FALSE	16
TRUE	26
Total	43

Source: Aliyu M.A, Istanbul 2015.

Table 2.11 shows the numerical representation of figure 2.10. Out of 43 students whom took part in the survey, one of the students gave an invalid response which was not tallied in the result, 16 answered False while 26 answered True. A percentile representation of both table 2.11 and figure 2.10 shows that 2.33percent of the students answered with a none valid answer "Neither True nor False". 37.21percent answered, "False" and 60.47percent answered, "True".

Figure 2.11: How secure do you feel your computer is?



Source: Aliyu M.A, Istanbul 2015.

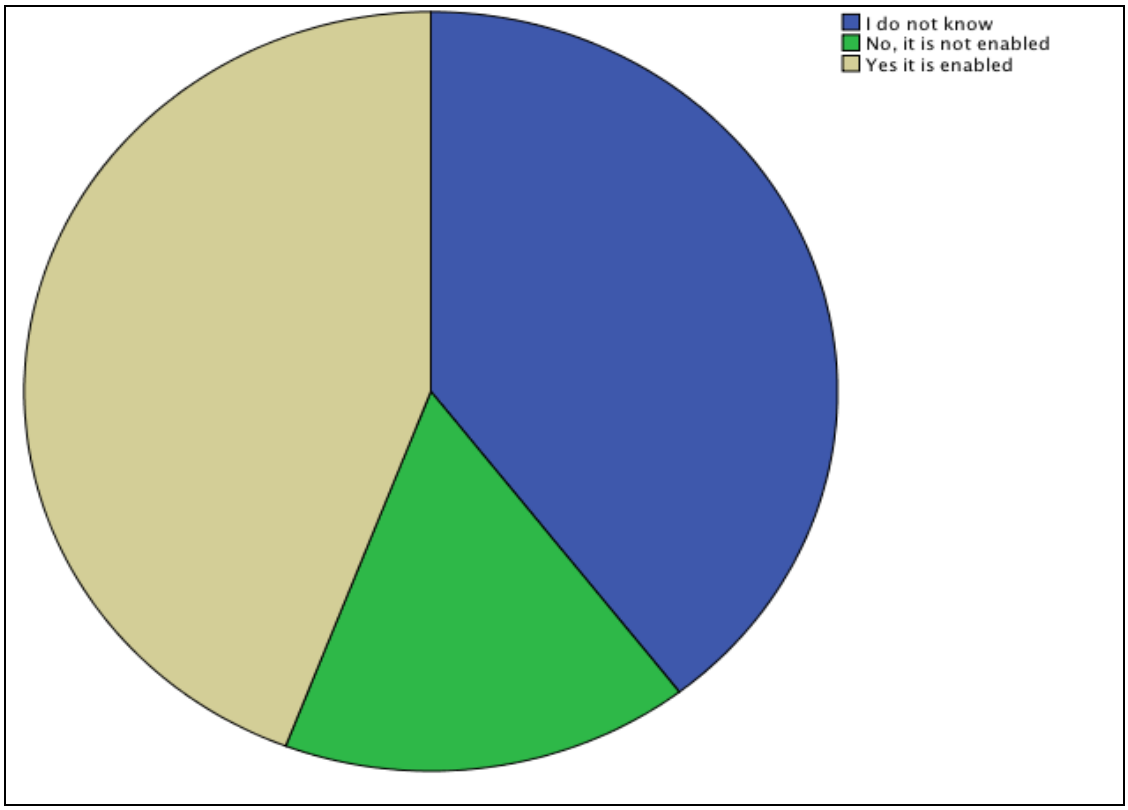
Table 2.12: Variable 10 Chat Statistics

Not Secure	16
Secure	24
Very Secure	3
Total	43

Source: Aliyu M.A, Istanbul 2015.

As seen in figure 2.11, students were asked to rate how secure they felt their computers to be. Table 2.12 shows that 16 of them, which is 37.21percent of them answered, "Not secure". 24 students, 55.81percent answered, "Secure" and 3 students, 6.98percent answered "Very Secure".

Figure 2.12: Is the firewall on your computer enabled?



Source: Aliyu M.A, Istanbul 2015.

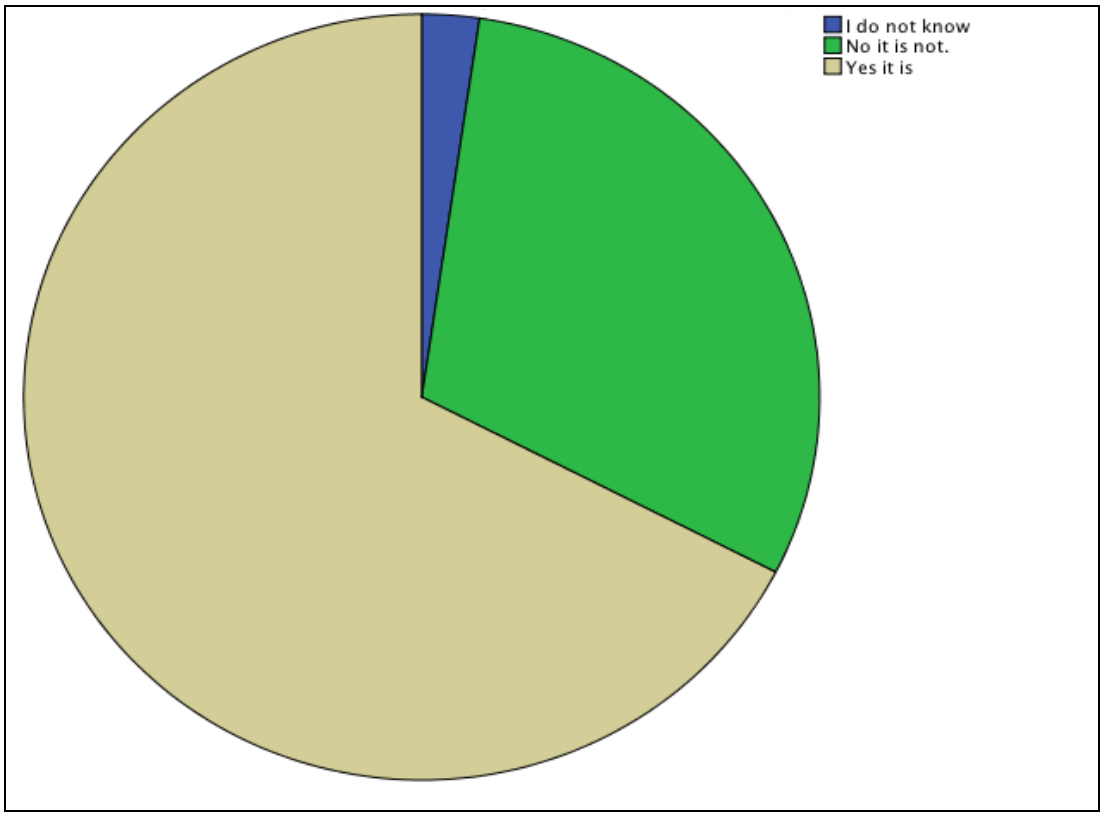
Table 2.13: Variable 11 Chat Statistics

I do not know	17
No, it is not enabled	7
Yes it is enabled	19
Total	43

Source: Aliyu M.A, Istanbul 2015.

Figure 2.12 depicts the response of students to the question; is firewall enabled on your computer? 39.53 percent of the students did not know if their firewall was enabled so they answered, "I do not know". 16.28 percent answered "No it is not enabled" and 44.19 percent answered, "Yes it is enabled". As seen in table 2.13 which is the numerical representation of response results shown in figure 2.12.

Figure 2.13: Is your computer configured to be automatically updated?



Source: Aliyu M.A, Istanbul 2015.

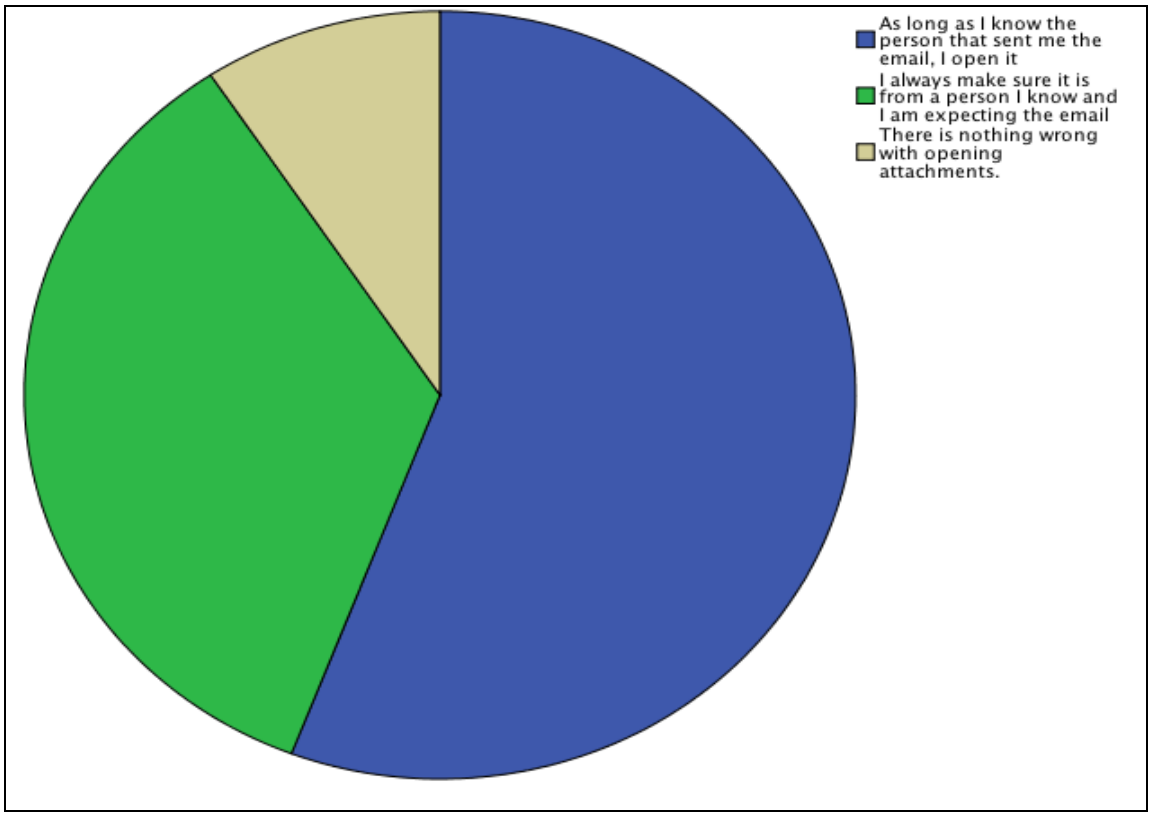
Table 2.14: Variable 12 Chat Statistics

I do not know	1
No it is not.	13
Yes it is	29
Total	43

Source: Aliyu M.A, Istanbul 2015.

As seen in figure 2.13, students were asked if their computers were automatically configured to be updated 2.33 percent did not know hence answered "I do not know", 30.23 percent answered "No it is not" and 67.44 percent answered "Yes it is". Table 2.14 shows the numerical representation of the responses in figure 2.13.

Figure 2.14: How careful are you when you open an attachment in email?



Source: Aliyu M.A, Istanbul 2015.

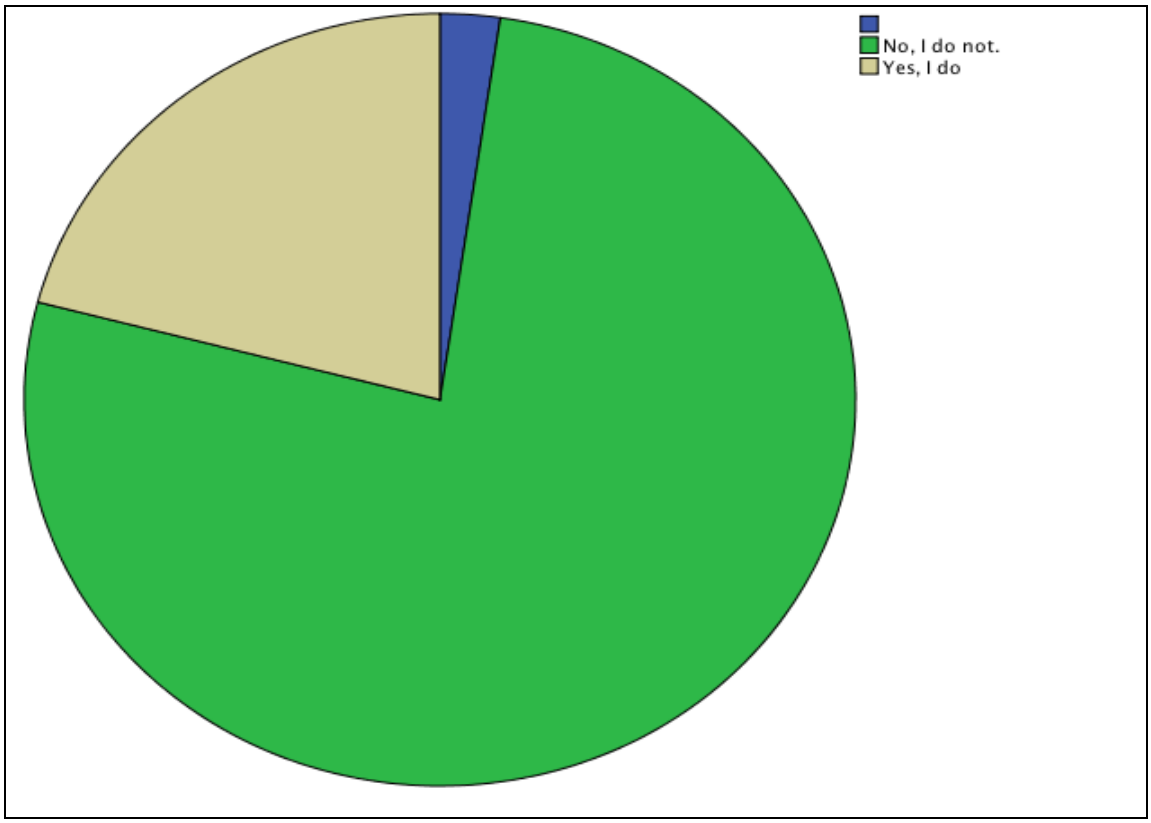
Table 2.15: Variable 13 Chat Statistics

As long as I know the person that sent me the email, I open it	24
I always make sure it is from a person I know and I am expecting the email	15
There is nothing wrong with opening attachments.	4
Total	43

Source: Aliyu M.A, Istanbul 2015.

Figure 2.14 asked the students in the survey, how careful are you when you open an attachment in email? 55.81 percent that is 24 students, as seen in table 2.15, which is a numerical representation of figure 2.14 answered, “As long as I know the person that sent me the email, I open it”. 15 students, 34.88 percent answered, “I always make sure it is from a person I know and I am expecting the email” and 4 students, 9.3 percent answered “There is nothing wrong with opening attachments.”

Figure 2.15: Do you know what phishing attack is?



Source: Aliyu M.A, Istanbul 2015.

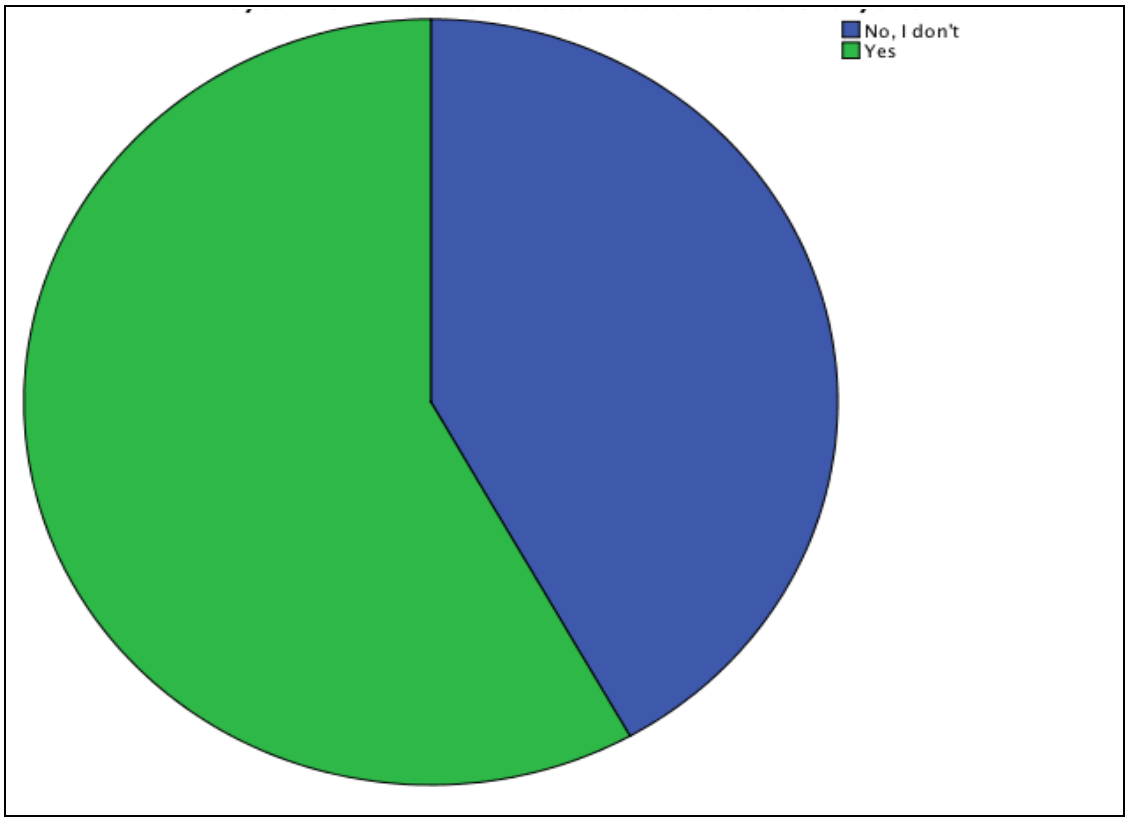
Table 2.16: Variable 14 Chat Statistics

None Valid	1
No, I do not.	33
Yes, I do	9
Total	43

Source: Aliyu M.A, Istanbul 2015.

Table 2.16, which is a numerical representation of figure 2.15 shows that when students were asked if they knew what phishing attack was 1 of the students, which is 2.33 percent of the students answered with a none valid answer (neither no, I do not nor Yes, I do). 33 of the students, 76.74 percent answered, "No, I do not" while 9 of the students, 20.93 percent knew what phishing attack was and answered, "Yes, I do".

Figure 2.16: Do you know what an email scam is and how to identify one?



Source: Aliyu M.A, Istanbul 2015.

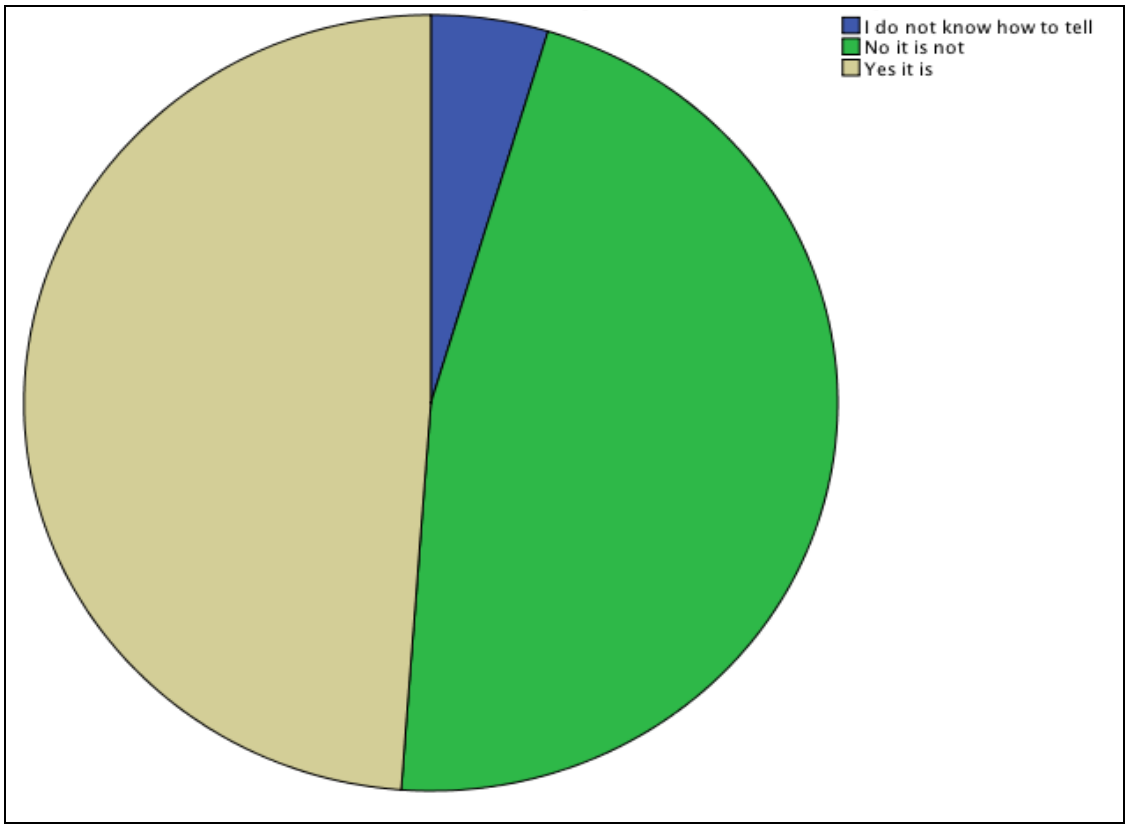
Table 2.17: Variable 15 Chat Statistics

No, I don't	18
Yes	25
Total	43

Source: Aliyu M.A, Istanbul 2015.

As seen in figure 2.16, students were asked if they knew what an email scam was and how to identify one, 41.86 percent answered, "No, I don't" while 58.14 percent, answered, "Yes". Table 2.17 shows a numerical representation of figure 2.16.

Figure 2.17: Is antivirus currently installed, updated and enabled on your computer?



Source: Aliyu M.A, Istanbul 2015.

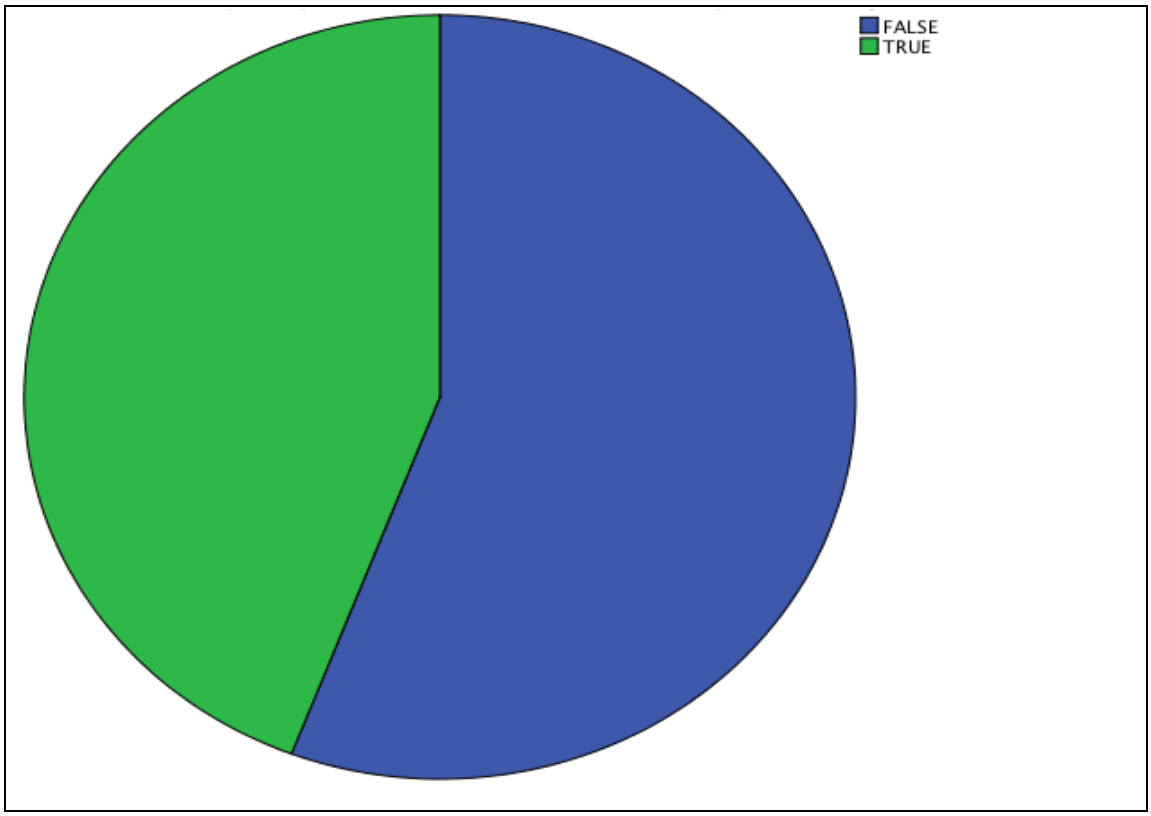
Table 2.18: Variable 16 Chat Statistics

I do not know how to tell	2
No it is not	20
Yes it is	21
Total	43

Source: Aliyu M.A, Istanbul 2015.

In figure 2.17, students were asked if their antivirus was currently installed, updated and enabled on their computer? 2 of the students, as seen in table 2.18 which is a numerical representation of figure 2.16, did not know how to identify if their antivirus was installed, updated and enabled answered "I do not know how to tell" that is 4.65 percent of the students. 20 students, 46.51 percent answered, "No, it is not" and 21 students, 48.84 percent answered, "Yes it is".

Figure 2.18: My computer has no value to hackers they will not target me.



Source: Aliyu M.A, Istanbul 2015.

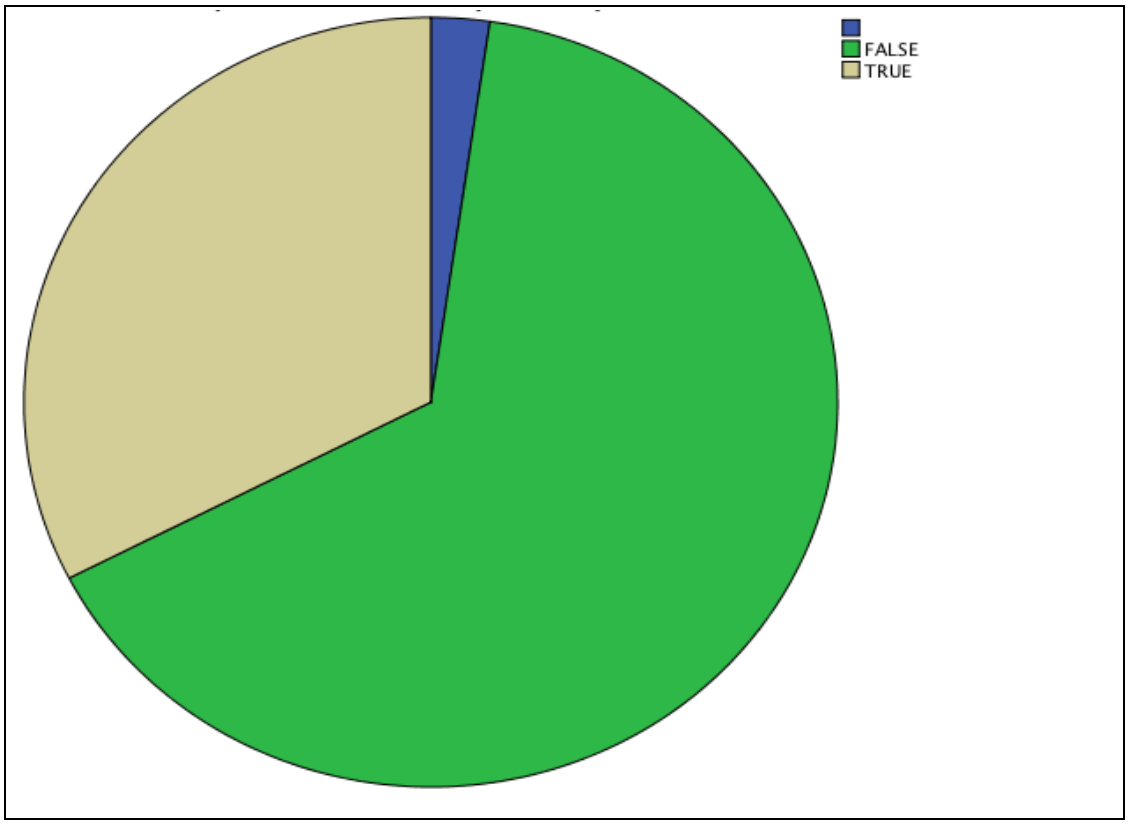
Table 2.19: Variable 17 Chat Statistics

FALSE	24
TRUE	19
Total	43

Source: Aliyu M.A, Istanbul 2015.

In figure 2.18, it depicts the answers students chose when given the statement "My computer has no value to hackers, they will not target me". 55.81 percent of the students did not believe they will not be targeted because they assumed their computers had no value to hackers, they admitted they were at a risk and answered "False" while 44.19 percent of the students believed they would not be targeted hence answered "True". Table 2.19 shows a numerical representation of the figure 2.18.

Figure 2.19: If you delete a file from your computer or USB stick that information is lost.



Source: Aliyu M.A, Istanbul 2015.

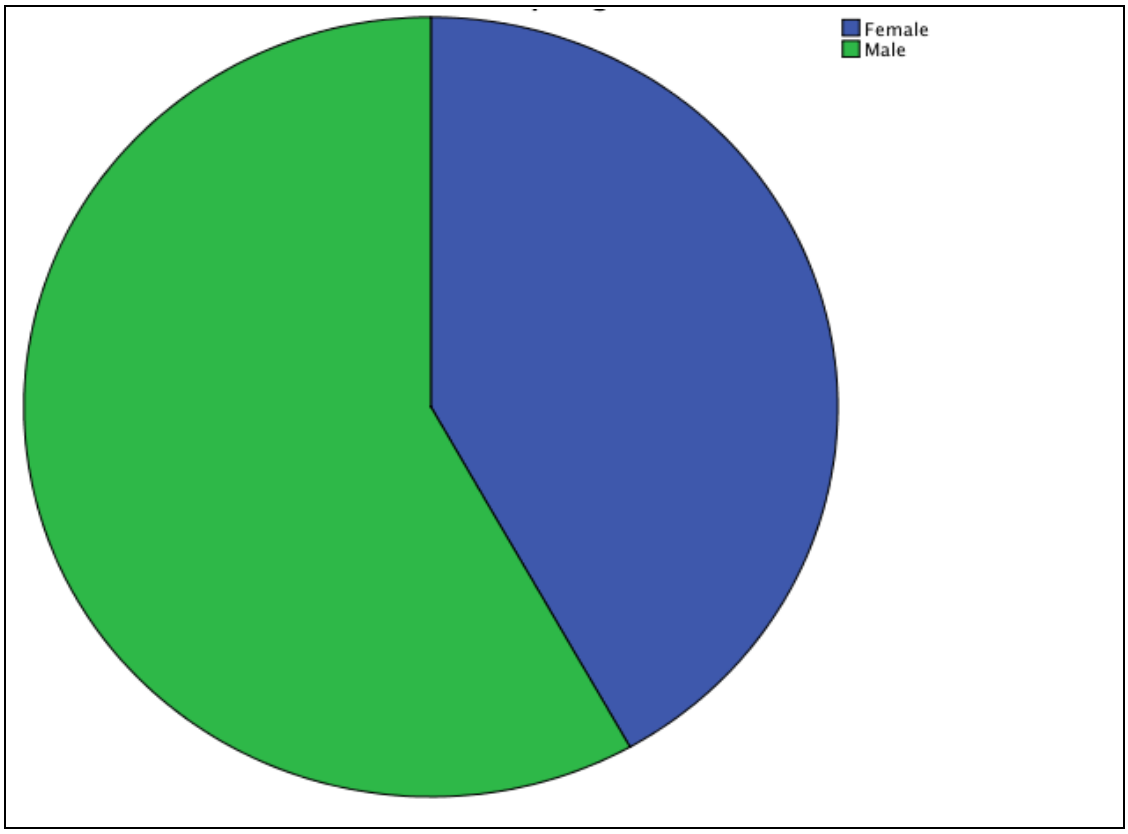
Table 2.20: Variable 18 Chat Statistics

None Valid	1
FALSE	28
TRUE	14
Total	43

Source: Aliyu M.A, Istanbul 2015.

In figure 2.19, students were given the statement that if a file was deleted from their computer or USB stick that information is lost. They were given the options true or false to agree or disagree with the statement, 2.33 percent of the students answered with a none valid answer which is neither true nor false. 65.12 percent answered “False” because they did not agree with this and 32.56 percent answered, “True” in agreement with this statement. Table 2.20 shows a numerical representation of the figure 2.19.

Figure 2.20: What is your gender?



Source: Aliyu M.A, Istanbul 2015.

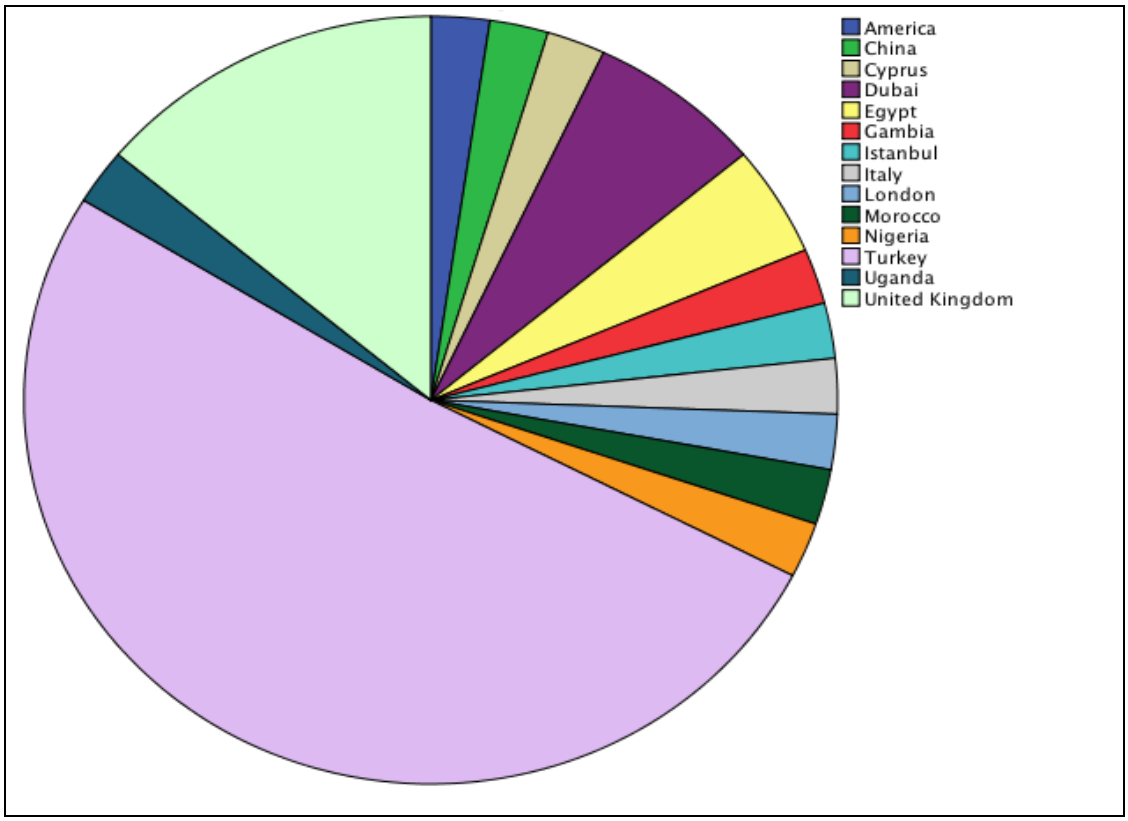
Table 2.21: Variable 19 Chat Statistics

Female	18
Male	25
Total	43

Source: Aliyu M.A, Istanbul 2015.

To be able to classify the results of the survey, figure 2.20, students were asked to supply their genders. 41.86 percent of the participants were Female while 58.14 percent of the participants were Male. Table 2.21 shows a numerical representation of the figure 2.20. 18 female students and 25 male students took part in the survey.

Figure 2.21: Where do you school (Location)?



Source: Aliyu M.A, Istanbul 2015.

Table 2.22: Variable 20 Chat Statistics

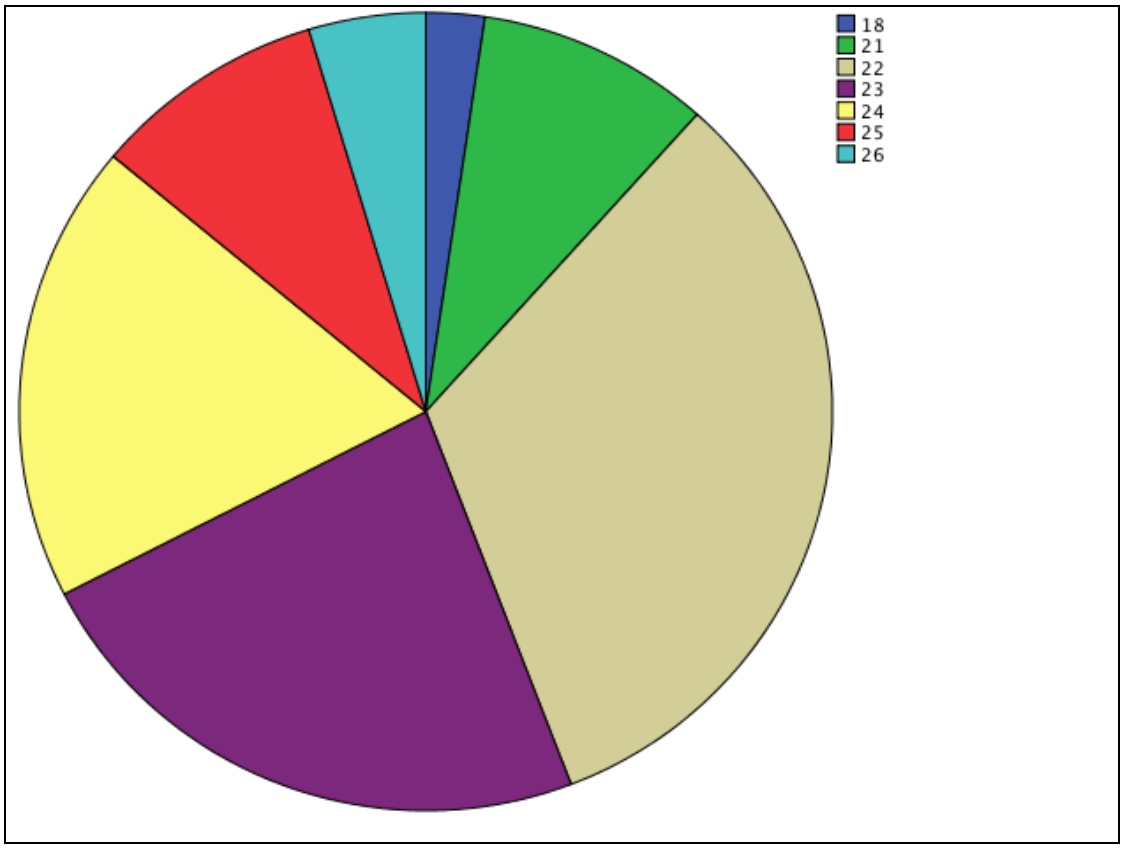
America	1
China	1
Cyprus	1
Dubai	3
Egypt	2
Gambia	1
Istanbul	1
Italy	1
London	1
Morocco	1
Nigeria	1
Turkey	22

Uganda	1
United Kingdom	6
Total	43

Source: Aliyu M.A, Istanbul 2015.

Since location of educational background was also a factor in the survey, figure 2.21, students were asked to supply the survey with their Locations (where they study). 2.33 percent of the students, which is 1 student was from America; 1 student from China took up another 2.33 percent. 1 student from Cyprus also had a frequency of 2.33 percent. 3 students that studied in Dubai had a 6.98 percent frequency. 2 students, 4.65 percent were from Egypt, another 2.33 percent each (1 student each) from Gambia, Istanbul, Italy, London, Morocco, Nigeria and Uganda. 22, which is 51.16 percent of the students were from Universities all over Turkey other than Istanbul and 6 students, 13.95 percent studied in the United Kingdom as seen in table 2.22 which is a numerical representation of figure 2.21.

Figure 2.22: What is your age?



Source: Aliyu M.A, Istanbul 2015.

Table 2.23: Variable 21 Chat Statistics

18	1
21	4
22	14
23	10
24	8
25	4
26	2
Total	43

Source: Aliyu M.A, Istanbul 2015.

Figure 2.22 depicts the ages of the students whom participated in the survey. Age was also a determinant factor in devising the bases of the survey results. 1 student, as seen in

table 2.23, which is a numerical representation of figure 2.22, was 18 years old meaning 2.33 percent of 43 students. 9.30 percent of the students were 21 years old, which is 4 students. 32.56 percent of the students were 22 years old (14 students), 23.26 percent of the students were 23 years old (10 students). 18.60 percent of the students were 24 years old (8 students), 9.30 percent were 25 years old (4 students) and 4.65 percent of the students were 26 years old (2 students).

2.4.1.2 Pre-test statistical data

Table 2.24 depicts the statistical data that represents the variables in this survey. Each row has a number of valid and missing variables. It consists of a mean, standard deviation, variance and the percentile of the variables.

Table 2.24: Statistics

		What is your department	Do you own a personal computer	Do you know about Information Security	If your computer is hacked can you do something about it	Do you know who to contact incase you are hacked or if your computer is infected	Have you ever found a virus or Trojan on your computer
N	Valid	43	43	43	43	43	43
	Missing	0	0	0	0	0	0

		Do you know how to tell if your computer is hacked or infected	Does anyone have your computer password	If you format a hard drive or erase the files on it all the information is lost	How secure do you feel your computer is	Is the firewall on your computer enabled	Is your computer configured to be automatically updated
N	Valid	43	43	43	43	43	43
	Missing	0	0	0	0	0	0

		How careful are you when you open an attachment in email	Do you know what phishing attack is	Do you know what an email scam is and how to identify one	Is anti virus currently installed updated and enabled on your computer	My computer has no value to hackers they will not target me	If you delete a file from your computer or USB stick that information is permanently lost
N	Valid	43	43	43	43	43	43
	Missing	0	0	0	0	0	0

		What is your gender	Where do you school (Location)	What is your age
N	Valid	43	43	43
	Missing	0	0	0

Source: Aliyu M.A, Istanbul 2015.

2.4.1.3 Pre-test data frequency

Statistically, frequencies mean the number of classifications or reactions. It's an essential statistical instrument that gives a feeling of how regularly particular response choices happen in a populace.

The frequency table, Table 2.25-Table 2.45, shows the frequency distribution with four columns labelled: Frequency, Percent, Valid Percent, and Cumulative Per cent.

Frequency: This reports the quantity of cases that fall into every class of the variable that is being analyzed.

Percent: This shows the percentage of the total cases (missing and non-missing) of the variable.

Valid Percent: This reports the percentage of the total cases but does not include missing cases if there is any.

Cumulative Percentage: This includes the percentages of every area from the highest point of the table to the base, coming full circle in 100 percent. This is more valuable when the variable of examination is ranked or ordinal, as it makes it simple to get a feeling of what percentage of cases fall beneath every rank.

Table 2.25: Frequency Table: What is your department?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Architecture	4	9.3	9.3	9.3
	Aviation management	1	2.3	2.3	11.6
	Business Administration	7	16.3	16.3	27.9
	Business Administration and Management	1	2.3	2.3	30.2
	Cinema & TV	2	4.7	4.7	34.9
	Computer Engineering	2	4.7	4.7	39.5
	Computer Science	1	2.3	2.3	41.9
	Computing	1	2.3	2.3	44.2
	Economics and Administrative sciences	1	2.3	2.3	46.5
	Electrical and Electronics engineering	1	2.3	2.3	48.8
	Electrical Engineering	1	2.3	2.3	51.2
	Finance	1	2.3	2.3	53.5
	Global Affairs	1	2.3	2.3	55.8
	Industrial Engineering	1	2.3	2.3	58.1
	Information Technology	1	2.3	2.3	60.5
	International Business and Trade	1	2.3	2.3	62.8
	International Relations	2	4.7	4.7	67.4
	International Relations and Political Sciences	1	2.3	2.3	69.8
	Law	1	2.3	2.3	72.1
	MBBS	1	2.3	2.3	74.4
	Media	1	2.3	2.3	76.7
	Medicine	3	7.0	7.0	83.7
	Nanotechnology and Bionanotechnology	1	2.3	2.3	86.0
	Political Sciences	3	7.0	7.0	93.0
	Psychology	1	2.3	2.3	95.3
	Social Science	1	2.3	2.3	97.7
	Software Engineering	1	2.3	2.3	100.0
	Total	43	100.0	100.0	

Source: Aliyu M.A, Istanbul 2015.

Table 2.26: Frequency Table: Do you own a personal computer?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	43	100.0	100.0	100.0

Source: Aliyu M.A, Istanbul 2015.

Table 2.27: Frequency Table: Do you know about Information Security?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	I know a little about it	24	55.8	55.8	55.8
	No, I do not	14	32.6	32.6	88.4
	Yes, I know a lot about Information Security	5	11.6	11.6	100.0
	Total	43	100.0	100.0	

Source Aliyu M.A, Istanbul 2015.

Table 2.28: Frequency Table: If your computer is hacked can you do something about it?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No, I cannot do anything about it	32	74.4	74.4	74.4
	Yes, I know what to do if my computer is hacked	11	25.6	25.6	100.0
	Total	43	100.0	100.0	

Source Aliyu M.A, Istanbul 2015.

Table 2.29: Frequency Table: Do you know who to contact incase you are hacked or if your computer is infected?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No, I do not know who to contact	16	37.2	37.2	37.2
	Yes, I know who to contact	27	62.8	62.8	100.0
	Total	43	100.0	100.0	

Source: Aliyu M.A, Istanbul 2015.

Table 2.30: Frequency Table: Have you ever found a virus or Trojan on your computer?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	I do not know what a virus or Trojan is	1	2.3	2.3	2.3
	No, my computer has never being infected	12	27.9	27.9	30.2
	Yes, my computer has being infected before	30	69.8	69.8	100.0
	Total	43	100.0	100.0	

Source: Aliyu M.A, Istanbul 2015.

Table 2.31: Frequency Table: Do you know how to tell if your computer is hacked or infected?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No, I cannot.	14	32.6	32.6	32.6
	Yes, I can tell if my computer is hacked or infected	29	67.4	67.4	100.0
	Total	43	100.0	100.0	

Source: Aliyu M.A, Istanbul 2015.

Table 2.32: Frequency Table: Does anyone have your computer password?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	23	53.5	53.5	53.5
	Yes	20	46.5	46.5	100.0
	Total	43	100.0	100.0	

Source: Aliyu M.A, Istanbul 2015.

Table 2.33: Frequency Table: If you format a hard drive or erase the files on it all the information is lost?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid		1	2.3	2.3	2.3
	FALSE	16	37.2	37.2	39.5
	TRUE	26	60.5	60.5	100.0
	Total	43	100.0	100.0	

Source: Aliyu M.A, Istanbul 2015.

Table 2.34: Frequency Table: How secure do you feel your computer is?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Not Secure	16	37.2	37.2	37.2
	Secure	24	55.8	55.8	93.0
	Very Secure	3	7.0	7.0	100.0
	Total	43	100.0	100.0	

Source: Aliyu M.A, Istanbul 2015.

Table 2.35: Frequency Table: Is the firewall on your computer enabled?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	I do not know	17	39.5	39.5	39.5
	No, it is not enabled	7	16.3	16.3	55.8
	Yes it is enabled	19	44.2	44.2	100.0
	Total	43	100.0	100.0	

Source: Aliyu M.A, Istanbul 2015.

Table 2.36: Frequency Table: Is your computer configured to be automatically updated?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	I do not know	1	2.3	2.3	2.3
	No it is not.	13	30.2	30.2	32.6
	Yes it is	29	67.4	67.4	100.0
	Total	43	100.0	100.0	

Source: Aliyu M.A, Istanbul 2015.

Table 2.37: Frequency Table: How careful are you when you open an attachment in email?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	As long as I know the person that sent me the email, I open it	24	55.8	55.8	55.8
	I always make sure it is from a person I know and I am expecting the email	15	34.9	34.9	90.7
	There is nothing wrong with opening attachments.	4	9.3	9.3	100.0
	Total	43	100.0	100.0	

Source: Aliyu M.A, Istanbul 2015.

Table 2.38: Frequency Table: Do you know what phishing attack is?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid		1	2.3	2.3	2.3
	No, I do not.	33	76.7	76.7	79.1
	Yes, I do	9	20.9	20.9	100.0
	Total	43	100.0	100.0	

Source: Aliyu M.A, Istanbul 2015.

Table 2.39: Frequency Table: Do you know what an email scam is and how to identify one?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No, I don't	18	41.9	41.9	41.9
	Yes	25	58.1	58.1	100.0
	Total	43	100.0	100.0	

Source: Aliyu M.A, Istanbul 2015.

Table 2.40: Frequency Table: Is antivirus currently installed updated and enabled on your computer?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	I do not know how to tell	2	4.7	4.7	4.7
	No it is not	20	46.5	46.5	51.2
	Yes it is	21	48.8	48.8	100.0
	Total	43	100.0	100.0	

Source: Aliyu M.A, Istanbul 2015.

Table 2.41: Frequency Table: My computer has no value to hackers they will not target me?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	FALSE	24	55.8	55.8	55.8
	TRUE	19	44.2	44.2	100.0
	Total	43	100.0	100.0	

Source: Aliyu M.A, Istanbul 2015.

Table 2.42: Frequency Table: If you delete a file from your computer or USB stick that information is permanently lost?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid		1	2.3	2.3	2.3
	FALSE	28	65.1	65.1	67.4
	TRUE	14	32.6	32.6	100.0
	Total	43	100.0	100.0	

Source: Aliyu M.A, Istanbul 2015.

Table 2.43: Frequency Table: What is your gender?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Female	18	41.9	41.9	41.9
	Male	25	58.1	58.1	100.0
	Total	43	100.0	100.0	

Source: Aliyu M.A, Istanbul 2015.

Table 2.44: Frequency Table: Where do you school (Location)?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	America	1	2.3	2.3	2.3
	China	1	2.3	2.3	4.7
	Cyprus	1	2.3	2.3	7.0
	Dubai	3	7.0	7.0	14.0
	Egypt	2	4.7	4.7	18.6
	Gambia	1	2.3	2.3	20.9
	Istanbul	1	2.3	2.3	23.3
	Italy	1	2.3	2.3	25.6
	London	1	2.3	2.3	27.9
	Morocco	1	2.3	2.3	30.2
	Nigeria	1	2.3	2.3	32.6
	Turkey	22	51.2	51.2	83.7
	Uganda	1	2.3	2.3	86.0
	United Kingdom	6	14.0	14.0	100.0
	Total	43	100.0	100.0	

Source: Aliyu M.A, Istanbul 2015.

Table 2.45: Frequency Table: What is your age?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	18	1	2.3	2.3	2.3
	21	4	9.3	9.3	11.6
	22	14	32.6	32.6	44.2
	23	10	23.3	23.3	67.4
	24	8	18.6	18.6	86.0
	25	4	9.3	9.3	95.3
	26	2	4.7	4.7	100.0
	Total	43	100.0	100.0	

Source: Aliyu M.A, Istanbul 2015.

2.5 SECURITY AWERENESS SURVEY POST-TEST PHASE

Following the pre-test analysis on the survey carried out in this study, a further post-test survey was carried out to determine the hypotheses stated out in this survey. The survey consisted of 103 other students whom were asked to voluntarily take part in the survey. The survey was posted on Google drive for duration of one week and students were asked to volunteer. Each student answered all 21 questions of the survey. They were students from different departments (as seen in table 2.47).

Table 2.46: Post-test Risk Value Score

Question Number	Risk Value Score
2	420
3	370
4	257
5	248
6	219
7	313
8	298
9	257
10	245
11	322
12	242
13	198
14	300
15	221
16	186
17	282
18	270
Cumulative Total	4658

Source: Aliyu M.A, Istanbul 2015.

Each questions risk value was multiplied by the number of times it was chosen by survey takers. Question 1,20 and 21 had no risk value, starting from Question 2-18; the response total of each question was gotten and tallied in table 2.46 above. This was used to obtain the cumulative risk total of the survey and determine the risk level of the students.

Table 2.47: List of Departments in Post-Test Survey

	Frequency
Advertisement	1
Architecture	6
Automobile Engineering	1
Aviation management	2
Biomedical Sciences	1
Business Administration	9
Business Administration and Management	1
Cinema & TV	4
Civil Engineering	1
Computer Education	1
Computer Engineering	4
Computer Science	1
Dentistry	2
Department of computing	1
Economics and Administrative sciences	1
Electrical and Electronics Engineering	1
Electrical Engineering	1
English	1
Entrepreneurship	1
Finance	3
Genetic Engineering	2
Global Affairs	2
History	2
Industrial Engineering	2
Information Technology	1
Interior Design	1
International Business and Finance	1
International Business and Trade	2
International Relations	3
International Relations and Political Sciences	1
Islamic Law	2
Islamic Studies	1
Law	3
Management	3
Mathematics	1
MBBS	1
Mechanical Engineering	1

Media	2
Medicine	4
Megatronics Engineering	1
Nanotechnology and Bionanotechnology	1
Physics	1
Piloting	1
Political Science and Public Administration	2
Political Sciences	3
Psychology	4
Public Administration	1
Public Relations	1
Research and Developmental Studies	1
Secretarial Studies	1
Social Science	1
Sociology	3
Software Engineering	3
Total	103

Source: Aliyu M.A, Istanbul 2015.

Table 2.47 shows the total number of departments the students studied in and the frequency, that is, the amount of students from each department whom took part in the post-test survey.

2.5.1 Cronbach Alpha

Cronbach Alpha is an estimation of the internal consistency (how closely related items are as a group) that is associated with the scores that can be derived from a scale or a composite score. It is usually done before statistical operations are performed using a dataset. Reliability reinforces the validity with the score.

The Cronbach alpha coefficient for the 16 numerical items tested is ($\alpha = .740$) (74 percent internally reliable variance). The following component variable has zero variance and it was removed from the scale: Do you own a personal computer?

Cronbach's Alpha based on Standardized Items is different Cronbach's alpha because it measures the reliability assuming all items have the same variance for the 16 numerical

items tested is (α = .717) (approximately 72 percent internally reliable variance) (see table 2.48).

Table 2.48: Cronbach Alpha

Reliability Statistics		
Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.740	.717	16

Source: Aliyu M.A, Istanbul 2015.

3. FINDINGS

3.1 SECURITY AWERENESS SURVEY PRE-TEST PHASE RESULTS

The cumulative response of 43 students from the survey was evaluated and their risk values computed. The total Risk Value of students was calculated by dividing the cumulative total by the total number of survey takers.

Risk Value= Cumulative Total/43 =2216/43 = 52

Using the table 2.1, the risk level of students was determined as **Average** based on the risk value**.** This means that students are aware of security threats; they have no knowledge of security standards and policies but also do not take any measures against them or take part in activities that put them at risk. Students need more studies on Information security so as to be aware of looming threats. They may not think they are at a risk now, but without this awareness, students would grow on to have careers and businesses which without this knowledge will put them at a great risk as new form of security threats are emerging everyday.

3.1.1 Pre-test Survey Case Processing

To be able to prove the hypotheses put forward in this study, a cross-tabular analysis was carried out which weighted the variables that formed our hypotheses against the students' perception of their knowledge of information security awareness. Table 3.1 is a case-processing summary to prove that all 43 students whom took part in this survey were used as valid cases in this analysis. There were no missing cases.

Table 3.1: Case Processing Summary

	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
What is your department * Do you know about Information Security?	43	100.0 percent	0	0.0 percent	43	100.0 percent
Where do you school (Location) * Do you know about Information Security?	43	100.0 percent	0	0.0 percent	43	100.0 percent
What is your gender * Do you know about Information Security?	43	100.0 percent	0	0.0 percent	43	100.0 percent
What is your age * Do you know about Information Security?	43	100.0 percent	0	0.0 percent	43	100.0 percent

Source: Aliyu M.A, Istanbul 2015.

3.1.2 Pre-Test Cross Tabulation Results

Survey output was based on a cross tabulation analysis done with IBMs SPSS software. To determine what factors affected the students' knowledge of Information security, an analysis was made, which used the students Department, Gender, Location and Age as the bases of the analysis. The columns in the tables contained the variables that the students answered and the rows contained the determinant factors that would be used to draw up the results of the survey as given in Table 3.2 to Table 3.5.

3.1.2.1 Statistical results

According to the frequency output, out of the 43 participants of the survey, 24 of the students answered, "I know a little about Information Security", 14 answered "No I do not know about Information Security" and 5 answered, "I know a lot about Information Security". It means that 11.62 percent of the students know a lot about Information Security, but, 55.81 percent of the students know a little about Information Security and 32.55 percent of the students do not know about Information Security.

Table 3.2 weighted the students department against their answer for the variable, "Do you know about Information Security?"

According to the data presented in this analysis, 80 percent of the 5 students that knew a lot about information security study in technology related departments and 20 percent from Political Sciences. Out of the 38 students that knew a little to nothing about

Information Security, 13.15 percent of the students study in Technology/Engineering Departments while 86.85 percent study in the Social Science departments. This proves the hypothesis that department is a determinant factor for the information security awareness levels of students.

Table 3.2: What is your department * Do you know about Information Security Cross tabulation

Count					
		Do you know about Information Security			Total
		I know a little about it	No, I do not	Yes, I know a lot about Information Security	
What is your department	Architecture	3	1	0	4
	Aviation management	1	0	0	1
	Business Administration	5	2	0	7
	Business Administration and Management	1	0	0	1
	Cinema & TV	1	1	0	2
	Computer Engineering	1	0	1	2
	Computer Science	0	0	1	1
	Computing	0	0	1	1
	Economics and Administrative sciences	0	1	0	1
	Electrical and Electronics engineering	0	1	0	1
	Electrical Engineering	0	1	0	1
	Finance	1	0	0	1
	Global Affairs	1	0	0	1
	Industrial Engineering	0	1	0	1
	Information Technology	1	0	0	1
	International Business and Trade	0	1	0	1
	International Relations	0	2	0	2
	International Relations and Political Sciences	1	0	0	1
	Law	1	0	0	1
	MBBS	1	0	0	1
	Media	0	1	0	1
	Medicine	3	0	0	3
	Nanotechnology and Bio nanotechnology	0	0	1	1
	Political Sciences	1	1	1	3
	Psychology	0	1	0	1
	Social Science	1	0	0	1

	Software Engineering	1	0	0	1
Total		24	14	5	43

Source: Aliyu M.A, Istanbul 2015.

Table 3.3 shows the students' location against their answer for the variable, "Do you know about Information Security?" 40 percent of the 5 students that knew a lot about Information Security study in the United Kingdom, 20 percent in America, 20 percent in China and 20 percent in Turkey. Furthers analysis tests would be need to prove the hypothesis being referred to here. In the post-test evaluation survey phase, this paper will try to prove that location is a determinant factor in the information security awareness level of students.

Table 3.3: Where do you school (Location) * Do you know about Information Security Cross tabulation

Count					
		Do you know about Information Security			**Total**
		I know a little about it	**No, I do not**	**Yes, I know a lot about Information Security**	
Where do you school (Location)	America	0	0	1	1
	China	0	0	1	1
	Cyprus	0	1	0	1
	Dubai	1	2	0	3
	Egypt	2	0	0	2
	Gambia	1	0	0	1
	Istanbul	1	0	0	1
	Italy	1	0	0	1
	London	1	0	0	1
	Morocco	1	0	0	1
	Nigeria	0	1	0	1
	Turkey	13	8	1	22
	Uganda	1	0	0	1
	United Kingdom	2	2	2	6
Total		24	14	5	43

Source: Aliyu M.A, Istanbul 2015.

Table 3.4 weighted the students' gender against their answer for the variable, "Do you know about Information Security?"

The 18 (41.86 percent) of the students were female and 25 (58.13 percent) of the students were male. 40 percent of the 5 students that know a lot about Information Security were female while 60 percent of them were male. The 42.11 percent of the students whom knew nothing to a little about Information Security were female while 57.89 percent of them were male. There is not enough evidence to support the hypothesis here.

Table 3.4: What is your gender * Do you know about Information Security Cross tabulation

Count					
		Do you know about Information Security			Total
		I know a little about it	No, I do not	Yes, I know a lot about Information Security	
What is your gender	Female	11	5	2	18
	Male	13	9	3	25
Total		24	14	5	43

Source: Aliyu M.A, Istanbul 2015.

Table 3.5 describes the students' age against their answer for the variable, "Do you know about Information Security?"

The average age of the students whom participated in the survey is 22. The minimum age of the students was 18 and the maximum age was 26.

The 44.18 percent of the students whom participated in the survey were between the ages of 18-22 while 55.81 percent of the students were between ages of 23-26.

The 60 percent of the 5 students whom knew a lot about Information security were between the ages of 23-26 while 40 percent were between the ages of 18-22.

The 44.73 percent of the 38 students whom knew a little to nothing about Information Security were between the ages of 18-22 while the 55.26 percent of them were between the ages of 23-26. It proves that the adult students have higher information security awareness levels than the younger students.

Table 3.5: What is your age * Do you know about Information Security Cross tabulation

Count					
		Do you know about Information Security			Total
		I know a little about it	No, I do not	Yes, I know a lot about Information Security	
What is your age	18	0	1	0	1
	21	1	2	1	4
	22	10	3	1	14
	23	4	5	1	10
	24	5	1	2	8
	25	2	2	0	4
	26	2	0	0	2
Total		24	14	5	43

Source: A. M Aliyu. Istanbul 2015

3.2 SECURITY AWERENESS SURVEY POST-TEST PHASE RESULTS

The cumulative response of 103 students from the survey was evaluated and risk values were computed for each in the post-test evaluation phase. The total Risk Value of students was calculated by dividing the cumulative total by the total number of survey takers.

Risk Value= Cumulative Total/103= 4658/103 =45

Using the table 2.1, the risk level of students was determined as **Below Average.** This means that students are aware of security threats, have knowledge of security policies and standards but do not apply them. Students need more studies on Information security standards and how to protect themselves. Prior pre-test showed us that students were at an average risk level that they had knowledge of information security threats but were not aware of security standards and policies. The post-test analysis proves that students' awareness level is at an incline, students are getting to know more about information security policies and standards and soon will be able to protect themselves against threats and significantly reduce their risk levels.

3.2.1 Post-test Survey Case Processing

To be able to further prove the hypotheses put forward in this study, during the process of post-test analysis, a cross-tabular analysis was also carried out which weighted the variables that formed our hypotheses against the students' perception of their knowledge of information security. Table 3.6 is a case-processing summary to prove that all 103 students whom took part in this survey were used as valid cases in this analysis. There were no missing cases.

Table 3.6: Post-Test Case Processing Summary

	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
What is your department * Do you know about Information Security?	103	100.0 percent	0	0.0 percent	103	100.0 percent
Where do you school (Location) * Do you know about Information Security?	103	100.0 percent	0	0.0 percent	103	100.0 percent
What is your gender * Do you know about Information Security?	103	100.0 percent	0	0.0 percent	103	100.0 percent
What is your age * Do you know about Information Security?	103	100.0 percent	0	0.0 percent	103	100.0 percent

Source: Aliyu M.A, Istanbul 2015.

3.2.2 Post-Test Cross Tabulation Results

First post-test survey output was based on a cross tabulation analysis that was used to determine what factors affected the students' knowledge of Information security, an analysis was made, which used the students' department, gender, location and age as the bases of the analysis. The columns in the tables contained the variables that the students answered and the rows contained the determinant factors that would be used to draw up the results of the survey as given in Table 3.7-3.10.

3.2.2.1 Statistical results

According to the frequency output, out of the 103 participants of the survey, 40 of the students answered, “I know a little about Information Security”, 50 answered “No I do not know about Information Security” and 13 answered, “Yes, I know a lot about Information Security”. The 12.62 percent of the students know a lot about Information Security. The 38.83 percent of the students know a little about Information Security and the 48.54 percent of the students do not know about Information Security.

Table 3.2 weighted the students department against their answer for the variable, “Do you know about Information Security?”

According to the data presented in this analysis, the 76.92 percent of the 13 students that knew a lot about information security study in Technology related departments and the 23.08 percent from Political Sciences. The 27 students were from technology related departments while 76 were from nontechnology related departments. Out of 27, 37.03 percent knew a lot about information technology, the 25.92 percent knew a little about Information Security and only the 37.05 percent knew nothing about Information Security.

Out of the 90 students that knew a little to nothing about Information Security, only the 25.56 percent of the students study in Technology/Engineering Departments. The 74.44 percent study in the nontechnology related departments, these are the students are a higher risk than the other groups. There is a significant margin among the classes of students (those in technology departments and otherwise) which proves that department is a determinant factor in the information security levels of students.

Table 3.7: What is your department * Do you know about Information Security Cross tabulation

Count					
		Do you know about Information Security			**Total**
		Yes, I know a lot about Information Security	**No, I do not**	**I know a little about it**	
What is your department	Advertisement	0	1	0	1
	Architecture	1	1	4	6
	Automobile Engineering	1	0	0	1

	Aviation management	1	0	1	2
	Biomedical Sciences	0	0	1	1
	Business Administration	0	2	7	9
	Business Administration and Management	0	1	0	1
	Cinema & TV	0	2	2	4
	Civil Engineering	0	0	1	1
	Computer Education	1	1	0	1
	Computer Engineering	1	0	3	4
	Computer Science	1	0	0	1
	Dentistry	0	1	1	2
	Department of computing	1	0	0	1
	Economics and Administrative sciences	0	1	0	1
	Electrical and Electronics Engineering	0	1	0	1
	Electrical Engineering	0	1	0	1
	English	0	1	0	1
	Entrepreneurship	0	0	1	1
	Finance	0	1	2	3
	Genetic Engineering	0	2	0	2
	Global Affairs	0	1	1	2
	History	2	0	0	2
	Industrial Engineering	0	1	1	2
	Information Technology	0	0	1	1
	Interior Design	1	0	0	1
	International Business and Finance	0	1	0	1
	International Business and Trade	0	1	1	2
	International Relations	0	2	1	3
	International Relations and Political Sciences	0	1	0	1
	Islamic Law	0	2	0	2
	Islamic Studies	0	1	0	1
	Law	0	2	1	3
	Management	0	2	1	3

	Mathematics	0	1	0	1
	MBBS	0	0	1	1
	Mechanical Engineering	0	1	0	1
	Media	0	2	0	2
	Medicine	0	2	2	4
	Megatronics Engineering	0	1	0	1
	Nanotechnology and Bio nanotechnology	1	0	0	1
	Physics	0	1	0	1
	Piloting	1	0	0	1
	Political Science and Public Administration	0	1	1	2
	Political Sciences	0	1	2	3
	Psychology	0	3	1	4
	Public Administration	0	1	0	1
	Public Relations	0	1	0	1
	Research and Developmental Studies	0	1	0	1
	Secretarial Studies	0	1	0	1
	Social Science	0	1	0	1
	Sociology	0	2	1	3
	Software Engineering	1	0	2	3
Total		13	50	40	103

Source: Aliyu M.A, Istanbul 2015.

Table 3.7 weighted the students' location against their answer for the variable, "Do you know about Information Security?"

The 16.50 percent of the students knew a lot about information security. The 5.88 percent each of the students whom knew a lot about IS were from Bangladesh, Canada, Dubai,

India, Italy, Morocco, Niger, Palestine, and United Kingdom while the 11.76 percent each were from Cameroun, China, Nigeria and Turkey respectively. Turkey had the highest number of survey participant hence highest amount of students whom knew about information security. This is not enough to prove hypothesis. There is an unequal distribution of frequencies; an ANOVA test hence would be necessary to prove the hypothesis put forward in this study. A cross-tabulation analysis would not be able to prove the hypothesis which states that the location of students is a determinant factor in the information security awareness level of students.

Table 3.8: Where do you school (Location) * Do you know about Information Security Cross tabulation

Count					
		Do you know about Information Security			
		Yes, I know a lot about Information Security	**No, I do not**	**I know a little about it**	**Total**
Where do you school (Location)	America	0	4	4	8
	Bangladesh	1	0	0	1
	Cameroun	2	1	0	3
	Canada	1	2	3	6
	China	2	2	0	4
	Cyprus	0	1	0	1
	Dubai	1	2	0	3
	Egypt	0	0	2	2
	Gambia	0	0	1	1
	India	1	2	1	4
	Italy	1	0	0	1
	Morocco	1	0	1	2
	Niger	1	1	0	2
	Nigeria	2	4	0	6
	Palestine	1	0	1	2
	South Africa	0	1	2	3
	Turkey	2	12	16	30
	UAE	0	3	5	8
	Uganda	0	0	1	1
	United Kingdom	1	8	6	15

Total	17	17	43	43	103

Source: Aliyu M.A, Istanbul 2015.

Table 3.9 weighted the students' gender against their answer for the variable, "Do you know about Information Security?"

The 46 (44.66 percent) of the students were female and 57 (55.34 percent) of the students were male. The 40 percent of the 5 students that know a lot about Information Security were female while 60 percent of them were male. The 54.17 percent of the female students knew about information security while the 45.83 percent of them were male students.

The 40.74 percent of the students whom knew nothing to a little about Information Security were female while the 59.26 percent of them were male. Cross-tabulation shows no significant margin between male students and female students.

Table 3.9: What is your gender * Do you know about Information Security Cross tabulation

Count					
		Do you know about Information Security			**Total**
		Yes, I know a lot about Information Security	**No, I do not**	**I know a little about it**	
What is your gender	Female	13	21	12	46
	Male	9	26	22	57
Total		22	47	34	103

Source: Aliyu M.A, Istanbul 2015.

Table 3.10 weighted the students' age against their answer for the variable, "Do you know about Information Security?"

The average age of the students whom participated in the survey is 22. The minimum age of the students was 18 and the maximum age was 26.

The 44.66 percent of the students whom participated in the survey were between the ages of 18-22 while the 55.34 percent of the students were between ages of 23-26. The 65.38 percent of the 26 students whom knew a lot about Information security were between the ages of 23-26 while the 34.62 percent were between the ages of 18-22.

The 48.05 percent of the 77 students whom knew a little to nothing about Information Security were between the ages of 18-22 while 51.95 percent of them were between the ages of 23-26. The older students seemed to have more knowledge of information security which supports the hypothesis here. To be able to further prove the hypothesis an ANOVA analysis would be needed to weigh the means of each age group and determine if the hypothesis has been supported.

Table 3.10: What is your age * Do you know about Information Security Cross tabulation

Count					
		Do you know about Information Security			Total
		Yes, I know a lot about Information Security	No, I do not	I know a little about it	
What is your age	18	1	0	0	1
	19	0	1	1	2
	20	1	6	0	7
	21	4	3	5	12
	22	3	8	13	24
	23	4	8	10	22
	24	6	5	4	15
	25	4	4	3	11
	26	3	2	4	9
Total		26	37	40	103

Source: A. M Aliyu. Istanbul 2015

3.2.2 ANOVA Results for Post-Test Phase

ANOVA analysis checks whether we have a statistically significant difference between group means. Students at the age of 20 showed the least amount of knowledge of significant information security (M=2.71, SD= 1.799) while others knew more than this group (see table 3.11 below), which agrees with hypothesis 1.

Table 3.11: Description of Hypothesis 1 (Age)

Do you know about Information Security?								
	N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
					Lower Bound	Upper Bound		
18	1	5.00	.	.	.	.	5	5
19	2	4.00	1.414	1.000	-8.71	16.71	3	5
20	7	2.71	1.799	.680	1.05	4.38	1	5
21	12	3.50	1.732	.500	2.40	4.60	1	5
22	24	3.50	1.216	.248	2.99	4.01	1	5
23	22	3.91	1.342	.286	3.31	4.50	1	5
24	15	3.27	1.486	.384	2.44	4.09	1	5
25	11	3.55	1.572	.474	2.49	4.60	1	5
26	9	3.89	1.453	.484	2.77	5.01	1	5
Total	103	3.56	1.439	.142	3.28	3.84	1	5

Source: Aliyu M.A, Istanbul 2015.

The main effect of the ages of students whom took part in the survey (between ages 18-26) on prior knowledge of information security was found to be, $F(8,94) = .741$, $p = .655$ (see table 3.12). Students between the ages of 21-26 showed more prior knowledge of information security than other group of students.

Table 3.12: Anova of Hypothesis 1 (Age)

Do you know about Information Security?					
	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	12.544	8	1.568	.741	.655
Within Groups	198.796	94	2.115		
Total	211.340	102			

Source: Aliyu M.A, Istanbul 2015.

There existed almost a statistically significant difference between the male students and female students, female students showed a .01 of significance more than the male students, which disproves hypothesis 2 (see table 3.13).

Table 3.13: Description of Hypothesis 2 (Gender)

Do you know about Information Security?							
	N	Mean	Std. Dev.	Std. Err.	95% Confidence Interval for Mean		Min	Max
					Lower Bound	Upper Bound		
Male	57	3.56	1.452	.192	3.18	3.95	1	5
Female	46	3.57	1.440	.212	3.14	3.99	1	5
Total	103	3.56	1.439	.142	3.28	3.84	1	5

Source: Aliyu M.A, Istanbul 2015.

The main effect of gender on prior knowledge of information security was F(1,101) = .000, p=0.989 (see table 3.14). Males (M = 3.56, SD = 1.452) and Females (M = 3.57, SD = 1.440).

Table 3.14: Anova of Hypothesis 2 (Gender)

Do you know about Information Security?					
	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	.000	1	.000	.000	.989
Within Groups	211.339	101	2.092		
Total	211.340	102			

Source: Aliyu M.A, Istanbul 2015.

A main effect of location on prior knowledge of information security was found to be, F (19, 83) = .964, p=.541 (see table 3.15).

Table 3.15: Description of Hypothesis 3 (Location)

Do you know about Information Security?								
	N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
					Lower Bound	Upper Bound		
United Kingdom	15	3.40	1.352	.349	2.65	4.15	1	5
Turkey	30	3.73	1.230	.225	3.27	4.19	1	5
Egypt	2	3.00	.000	.000	3.00	3.00	3	3
America	8	3.75	1.488	.526	2.51	4.99	1	5
Cyprus	1	5.00	.	.	.	.	5	5
Italy	1	3.00	.	.	.	.	3	3
Dubai	3	4.33	1.155	.667	1.46	7.20	3	5
Gambia	1	3.00	.	.	.	.	3	3
Uganda	1	3.00	.	.	.	.	3	3
Morocco	2	2.00	1.414	1.000	-10.71	14.71	1	3
China	4	3.00	2.309	1.155	-.67	6.67	1	5
Niger	2	5.00	.000	.000	5.00	5.00	5	5
Nigeria	6	3.67	2.066	.843	1.50	5.83	1	5
Palestine	2	2.00	1.414	1.000	-10.71	14.71	1	3
Canada	6	3.33	1.506	.615	1.75	4.91	1	5
India	4	4.00	2.000	1.000	.82	7.18	1	5
UAE	8	4.25	1.035	.366	3.38	5.12	3	5
Bangladesh	1	1.00	.	.	.	.	1	1
South Africa	3	3.67	1.155	.667	.80	6.54	3	5
Cameroun	3	2.33	2.309	1.333	-3.40	8.07	1	5
Total	103	3.56	1.439	.142	3.28	3.84	1	5

Source: Aliyu M.A, Istanbul 2015.

Participants from the Turkey, having the highest number of students reported significantly more prior information security knowledge (M=3.73, SD=1.230) than United Kingdom which had the second highest amount of students (M = 3.40, SD =1.352) (see table 3.16 below).

Table 3.16: Anova of Hypothesis 3 (Location)

	Do you know about Information Security?				
	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	38.206	19	2.011	.964	.510
Within Groups	173.133	83	2.086		
Total	211.340	102			

Source: Aliyu M.A, Istanbul 2015.

3.3 PRE-TEST RESULTS AND DISCUSSION

From the analysis, it has been concluded that out of the 38 students that knew a little to nothing about Information Security in the pre-test analysis discussed in section 2.2, the 13.15 percent of the students study in Technology/Engineering Departments while the 86.85 percent study in the Social Science departments hence, department highly affected the students knowledge of information security.

Students whom were already exposed to the computer and technologies proved to be more aware of information security, the risks and mitigation techniques while students from other departments proved to not be so aware of information security. This proves hypothesis four of this thesis mentioned in section 2. Due to the fact that there were only 1 student each from America, China, Gambia, Istanbul, Italy, London, Morocco, Nigeria. Location is not a determinant factor of students' knowledge of Information Security disproving hypothesis three. Gender has proven to not also be a determinant factor because the number of males and females in the survey were unequal and cross tabulation proved inconclusive hence, also disproving one more hypothesis, hypothesis 2. Age is a determinant factor because the 44.18 percent of the students whom participated in the survey were between the ages of 18-22 while the 55.81 percent of the students were between ages of 23-26. The older students proved to have higher IS awareness levels than the younger hypothesis 1.

Conclusively, hypothesis 4 which stated that the students department was a determinant of the level of awareness of the students and also hypothesis 1 which states that age is a determinant factor in the IS awareness level of students were the only valid hypothesis at

the end of the analysis procedure. There were 17 students from the sciences and technologies departments, 4 from the Arts and 22 from the social sciences. The department, which have a greater number of students whom know a little about IS was from the Arts and Social Sciences departments. Out of the 14 people that know nothing about information security, the 85.71 percent of them are from the Arts and Social Science departments. Students whom had background knowledge in the technologies fared well in the survey. They were the students whom knew a lot or a little about Information Security while a majority of the students from the Arts and Social sciences did not know about Information Security because they had zero to no training in it. Table 3.17 below depicts the outcomes of the hypotheses following the results of the pre-test survey.

Table 3.17: Outcome of hypotheses test in Pre-test Survey

	Hypotheses	**Outcome**	**Status**
Hypothesis 1	Age is a determinant factor in the IS awareness level of students.	**Supported**	**Validated**
Hypothesis 2	Gender is a determinant factor in the IS awareness level of students.	**Supported**	**Not Validated**
Hypothesis 3	Location of the university is a determinant factor in the IS awareness level of students.	**Supported**	**Not Validated**
Hypothesis 4	Department of students is a determinant factor in the IS awareness level of students.	**Supported**	**Validated**

Source: A. M Aliyu. Istanbul 2015

3.4 POST-TEST RESULTS AND DISCUSSION

To prove the hypotheses brought forward in this thesis, all analysis carried out were of outmost importance. The pre-test survey initially proved hypothesis 4, validating that department is a factor in determining the awareness level of students. In the post-test survey, it was proven that the younger students had better IS awareness levels than the older students, 22 being the median age proved this theory (see table 3.6). Gender was validated neither by the pre-test nor our post-test, it is however a supported hypothesis with a significant difference of almost 1. The ANOVA analysis also proved that location was a valid hypothesis as seen in table 3.12 below. Due to the fact that ANOVA analysis can only be carried out on numerical variables and not string variables, the hypothesis 3, which states department as a determinant factor for the IS awareness level of students was not put to the test hence, the result from the cross-tabulation analysis which weighted the students departments against their answers to survey question "Do you know about Information security" was used. The cross-tabulation statistics showed that a significant percentage of the students whom were from technology related departments had higher IS awareness levels. Although the cross-tabulation analysis proved that hypothesis 1 was valid, the ANOVA analysis result further proved this point.

Table 3.18 shows a table of outcome for the hypotheses put forward in this paper. All hypotheses were supported by the survey and survey analysis carried out, the table represents both the pre-test outcome and the post-test outcome.

Table 3.18: Outcome of hypotheses test in Post-test Survey

	Hypotheses	Outcome	Status
Hypothesis 1	Age is a determinant factor in the IS awareness level of students.	**Supported**	**Validated**
Hypothesis 2	Gender is a determinant factor in the IS awareness level of students.	**Supported**	**Not Validated**
Hypothesis 3	Location of the university is a determinant factor in the IS awareness level of students.	**Supported**	**Validated**
Hypothesis 4	Department of students is a determinant factor in the IS awareness level of students.	**Supported**	**Validated**

Source: A. M Aliyu. Istanbul 2015

4. CONCLUSION

Information security is a global issue in our growing society. In an age of technical revolution, where information is easily and readily accessible with the click of a mouse, our society needs to be more aware and conscious of the dangers that come with a digitalized world. Lack of security with the information we store on our virtual machines leads to a large number of collapsed businesses, sharing of private information and loss of vital information yearly. Students whom will grow up to be owners of large and small businesses need to be very educated about information security. In order to have a successful business/career in the next couple of years, students need to be educated about the risks that come with information technology and ways in which these risks can be mitigated. Schools need to add a mandatory Information Security class for all students (not just students in the technology departments), at a very primitive age. Almost every child has a digital device in today's world, it is only right for these kids to know that there information is at a risk if they do not have a knowledge of the risks and proper security standards and policies. Based on the survey carried out icvn this paper and the discussions in previous sections, it shows that students whom knew more about IS seemed to have higher self-efficacy levels. They are the students whom were aware of the danger of IS and whom either knew what to do about the security threats or knew whom to contact. Some of the students did not have a basic knowledge of whom to contact in any case where they find that their system has being compromised. These are the students with lower self-efficacy levels.

Deci and Ryan's theory of self-determination states that, self determination (SDT) is a theory of motivation. It is concerned with supporting our regular or inborn tendencies to act in successful and solid ways. The students whom were IS aware were more motivated to act in a secure a safe manner when using the personal computers.

The Theory of planned behavior, TPB (Icek Ajzen) pushes to understand how we can change people's behavior, it strives to demonstrate that people's behaviors are deliberate and behavior can be planned.

There are 3 considerations in the theory of planned behavior: Behavioral Beliefs is about the possible consequences of an action (behavior). Normative Beliefs is about the

normative expectations of others. Control Beliefs is about the presence of possible factors that may encourage or impede the performance of that action (behavior).

If students were security aware, if they had received some form of early training, they would be able use the beliefs stated in Icek Ajzens TPB to direct the course of their online security. TPBs behavioral beliefs prove that if students had prior knowledge of the consequences of their actions, they would stay away from such exploitative online activities, or those with a higher level of self-efficacy would end up finding ways to protect themselves.

REFERENCES

Books

Art B., Todd G.2013. *Investigating Internet Crimes.* Chapter 16: Detection and Prevention of Internet Crimes.

Chantler, A. 1996a. *The changing definition and image of hackers in popular discourse.* International Journal of the Sociology of Law, Vol. 24, pp. 229-51.

Diogo A., Liliana F., Joao V., Mario M., and Pedro R. 2014. *Emerging Trends in ICT Security.* Chapter 25: A Quick Perspective on the Current State in Cyber security.

Gordon, Lawrence, Martin Loeb, and William Lucyshyn. (2003). *Sharing Information on Computer Systems Security: An Economic Analysis.* Journal of Accounting and Public Policy. Vol. 22, pp. 461-485.

James F., Eugene Tucker. 4th Edition. *Risk Analysis and The Security Survey*.

Joseph M. *Computer Network Security and Cyber Ethics*. 4th Edition. 240 pages.

Marina H. *A Perspective On Achieving Information Security Awareness*.

Michael L., Greg S., Blake H., Shahan S., Jon G., Falcone ,A., Ryan S., Arion L. 2011. *Cyber Security Essentials.*.

Nikolai M., Djenana C. 2010. *System Assurance: Beyond Detecting Vulnerabilities*. 368 pages (Chapter 6: Knowledge of vulnerabilities as an element of cyber security argument.

P.W Singer, Allan F. 2013. *Cyber security and Cyberwar.*

Periodicals

Campbell, D, 2000. The spy in your server. *Guardian Unlimited.*

D. Dagon, 2005. Botnet Detection and Response, The Network is the Infection. in *OARC Workshop.*

EY's Global Information Security Survey 2014.

G. Schaffer, 2006. Worms and Viruses and Botnets, Oh My! : Rational Responses to Emerging Internet Threats. *IEEE Security & Privacy*.

Garfinkel, S. and Spafford, G, 1996. Practical UNIX and Internet Security, 2d ed., *O'Reilly and Associates, Sebastopol, CA*.

Goodell, J. 1996. The Cyber Thief and the Samurai, *Dell Publishing, New York, NY.*

K. K. R. Choo. March 2007. "Zombies and Botnets," Trends and issues in crime and criminal justice, no. 333, *Australian Institute of Criminology, Canberra*.

Lawrence A., Martin P., William L, Robert R. 2005. *CSI/FBI Computer Crime And Security Survey*

An Introduction to Computer Security: The NIST Handbook. *National Institute of Standards and Technology*. Special Publication 800-12, 1995.

Provos, N, (2004. "A virtual honeypot framework," in Proc. *13th USENIX Security Symposium*, pp. 1-14.

Greatfire.Org. Outllok Grim. Chinese Authorities Attack Microsoft https://en.greatfire.org/blog/2015/jan/outlook-grim-chinese-authorities-attack-microsoft

Other Publications

Alan D., William T. 1993. Issues in cybersecurity; understanding the potential risks associated with hackers/crackers. http://www.emeraldinsight.com/doi/abs/10.1108/09685220210436976 [accessed 1 February 2015].

Alexander M., Tanya B., Steven D., and Henry M., Department of Computer Science & Engineering University of Washington . A Crawler-based Study of Spyware on the Web. http://homes.cs.washington.edu [accessed 10 December 2014].

Burcu B. , Hasan C. , Izak B., 2010. Information Security Policy Compliance: An Emprical Study Of Rationality-Based Beliefs And Information Security Awareness. http://aisel.aisnet.org [accessed 8 November 2014].

Chee-Wooi T. , Manimaran, G. , Chen-Ching L. 2010. Cybersecurity for Critical Infrastructures: Attack and Defense Modeling. http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=5477189&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D5477189. [accessed 8 November 2014].

Digital Data Communications, 2015. http://www.ddcnow.com/2014/10/20/are-you-vulnerable-to-watering-hole-attacks/, [accessed 6 May 6, 2015].

DuPaul N., Spoofing Attack: IP, DNS & ARP. http://www.veracode.com/security/spoofing-attack, [accessed 6 May 6, 2015].

Feily, M. Shahrestani, A. , Ramadass, S. (2009). A Survey of Botnet and Botnet Detection. Retrieved from: http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=5210988&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D5210988 [accessed 8 November 2014].

Hogg J. 2014. Analyzing and mitigating cybersecurity risks faced by small businesses. http://search.proquest.com [accessed 8 November 2014].

Hyeun-Suk R., Cheongtag K., Young U., 2009. Self-efficacy in information security: Its influence on end users' information security practice behavior.

John R. Vacca, (2012). Computer and Information Security Handbook, 2nd Edition.

Chapter 4: Preventing System Intrusions. Michael West. http://www.safaribooksonline.com [accessed 4 November 2014].

Josh P., 2013. The Basics Of Web Hacking. Tools and Techniques to Attack the Web. http://sciencedirect.com [accessed 10 December 2014].

Julian J., Surya N., 2012. A Survey Of Emerging Threats in Cyber security. http://www.sciencedirect.com [accessed 4 November 2014].

Khandelwal S., 2014. Apple Icloud and Activation Hack :Allows Hackers to Unlock Stolen Devices. http://thehackernews.com/2014/05/apple-icloud-and-activation-lock-hacked.html [accessed 1 February 2015].

Lawrence A., Martin P., Tashfeen S. 2003. A framework for using insurance for cyber-risk management. http://dl.acm.org/citation.cfm?id=636774 [accessed 1 February 2015].

Malek B., Shloomo H., Salvatore J. 2008. A Survey of Insider Attack Detection Research.

Michael P., Brent R. 2006. Private Sector Cyber Security Investment Strategies: An Empirical Analysis.

Michael A., 2013. Institute For Security Technology Studies at Dartmouth College, Cyber Attacks During The War On Terrorism: A Predictive Analysis. http://www.sciencedirect.com [accessed 4 November 2014].

Microsoft, Spyware http://www.microsoft.com/security/pc-security/spyware-whatis.aspx, [accessed 6 May 2015].

Osterman Research Survery. Security Awareness Training Effectiveness Report, http://www.ostermanresearch.com/research.htm [accessed 11 December 2014].

Paul V., Ken A. October 2014. Get ahead of cybercrime.

Ralston P., Graham J., Hieb J., 2007. Cyber security Risk Assessment For SCADA and DCS Networks. http://www.sciencedirect.com [accessed 4 November 2014].

Reuter N., 2011. The Cybersecurity Dilemma. http://search.proquest.com [accessed 10 December 2014].

Rossi M., July 2001. International Risk Management Institute. Standalone e-commerce market survey. www.irmi.com/expert/ articles/rossi004chart.asp. [accessed 14 March 2015].

Robert L., Nora R., Sunny L., Doohwang L., 2015. Online Safety Strategies: A Content

Analysis and Theoretical Assessment.

Robert R., 2008. The latest results from the longest-running project of its kind. CSI Computer Crime & Security Survey.

Rouse M., 2007. Denial-Of-Service, http://searchsoftwarequality.techtarget.com/definition/denial-of-service [accessed 6 May 2015]

Rouse M., 2005, Bot. http://searchsoa.techtarget.com/definition/bot, [accessed 6 May 2015]

Schechter, Stuart. 2004. Computer Security Strength & Risk: A Quantitative Approach. *PhD thesis, Harvard University.*

Schulman, A. , 2001. The extent of systematic monitoring of employee e-mail and Internet use, *Workplace Surveillance Project at Foundation.*

Security Awerness Survey, 2012. http://www.securingthehuman.org/media/resources/business-justification/security-awareness-survey.pdf, [accessed 10 December 2014].

TechTerms Malware, 2005. http://techterms.com/definition/malware, [accessed 10 December 2014].

Timothy C. Summers, 2013. How Hackers Think: A study of cybersecurity experts and their mental models, *Case Western Reserve University*.

Schonewille and D.J. van Helmond 2006. The Domain Name Service as an IDS. Master's Project, University of Amsterdam, Netherlands, http://staff.science.uva.nl/~delaat/snb-2005-2006/p12/report.pdf [accessed 1 February 2015].

Stringhini G., 2014. Stepping Up the Cybersecurity Game: Protecting Online Services from Malicious Activity. Retrieved from http://search.proquest.com [accessed 8 November 2014].

Swati K. Apple iCloud and Activation Lock Hacked; Allows Users To Unlock Stolen Devices http://thehackernews.com/2014/05/apple-icloud-and-activation-lock-hacked.html [accessed 10 December 2014]

Teodor S. 2012. A framework and theory for cyber security assessments. http://www.sommestad.com [accessed 10 December 2014].

Zhuo L., 2010, Review and Evaluation Of Security Threats On The Communication

Networks In The Smart Grid.
http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5679551&tag=1 [accessed 11 December 2014].

APPENDICES

Appendix A.1 Survey Questions

1. What is your department?

   …….
2. Do you own a personal computer?
   a. Yes
   b. No
3. Do you know about Information Security?
   a. Yes, I know a lot about Information Security
   b. No, I do not
   c. I know a little about it
4. If your computer is hacked, can you do something about it?
   a. Yes, I know what to do if my computer is hacked
   b. No, I cannot do anything about it
5. Do you know who to contact in case you are hacked or if your computer is infected?
   a. Yes, I know who to contact
   b. No, I do not know who to contact
6. Have you ever found a virus or Trojan on your computer?
   a. Yes, my computer has being infected before
   b. No, my computer has never being infected
   c. I do not know what a virus or Trojan is
7. Do you know how to tell if your computer is hacked or infected?
   a. Yes, I can tell if my computer is hacked or infected.
   b. No, I cannot.
8. Does anyone have your computer password?
   a. Yes
   b. No
9. If you format a hard drive or erase the files on it all the information on it is permanently lost.

a. True
b. False

10. How secure do you feel your computer is?
    a. Very Secure
    b. Secure
    c. Not Secure
11. Is the firewall on your computer enabled?
    a. Yes it is enabled
    b. No, it is not enabled
    c. I do not know
12. Has your computer configured to be automatically updated?
    a. Yes it is.
    b. No it is not.
    c. I do not know.
13. How careful are you when you open an attachment in email?
    a. I always make sure it is from a person I know and I am expecting the email.
    b. As long as I know the person that sent me the email, I open it.
    c. There is nothing wrong with opening attachments.
14. Do you know what phishing attack is?
    a. Yes, I do.
    b. No, I do not.
15. Do you know what an email scam is and how to identify one?
    a. Yes
    b. No, I do not.
16. Is anti-virus currently installed, updated and enabled on your computer?
    a. Yes it is
    b. No it is not
    c. I do not know how to tell
    d. I do not know how to tell
17. My computer has no value to hackers, they will not target me.
    a. True
    b. False

18. If you delete a file from your computer or USB stick, that information can no longer be recovered.
    a. True
    b. False
19. What is you Gender?
    a. Male
    b. Female
20. Where do you school (Location)?

    …….
21. What is your age?

    …….