

EFFECTIVENESS OF A SECURITY PORTAL FOR IMPROVING STUDENTS'  
KNOWLEDGE AND SKILLS IN INFORMATION TECHNOLOGY (IT) SECURITY

A THESIS SUBMITTED TO  
THE GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES  
OF  
MIDDLE EAST TECHNICAL UNIVERSITY

BY

NILAY PANCAR

IN PARTIAL FULLFILLMENT OF THE REQUIREMENTS  
FOR  
THE DEGREE OF MASTER OF SCIENCE  
IN  
COMPUTER EDUCATION AND INSTRUCTIONAL TECHNOLOGY

SEPTEMBER 2014



Approval of the thesis:

**EFFECTIVNESS OF A SECURITY PORTAL FOR IMPROVING STUDENTS  
KNOWLEDGE AND SKILLS IN IT SECURITY**

submitted by **NİLAY PANCAR** in partial fulfillment of the requirements for the degree  
of **Master of Science in Computer Education and Instructional Technology**  
**Department, Middle East Technical University** by,

Prof. Dr. Canan Özgen  
Dean, Graduate School of **Natural Applied Sciences**

\_\_\_\_\_

Prof. Dr. Soner Yıldırım  
Head of Department, **Computer Edu. and Inst. Tech.**

\_\_\_\_\_

Assoc. Prof. Dr. Ömer Delialioğlu  
Supervisor, **Computer Edu. and Inst. Tech. Dept., METU**

\_\_\_\_\_

**Examining Committee Members**

Prof. Dr. Zahide Yıldırım  
Computer Edu. & Instruct. Tech. Dept., METU

\_\_\_\_\_

Assoc. Prof. Dr. Ömer Delialioğlu  
Computer Edu. & Instruct. Tech. Dept., METU

\_\_\_\_\_

Assist. Prof. Dr. Cengiz Savaş Aşkun  
Computer Edu. & Instruct. Tech. Dept., METU

\_\_\_\_\_

Assist. Prof. Dr. Halil Ersoy  
Computer Edu. & Instruct. Tech. Dept., Başkent Uni.

\_\_\_\_\_

Instructor Dr. Hasan Karaaslan  
Computer Edu. & Instruct. Tech. Dept., METU

\_\_\_\_\_

**Date:**

Sept. 15, 2014

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

Name, Last name: Nilay PANCAR

Signature :

## **ABSTRACT**

### **EFFECTIVENESS OF A SECURITY PORTAL FOR IMPROVING STUDENTS KNOWLEDGE AND SKILLS IN IT SECURITY**

Pancar, Nilay

M.S., Department of Computer Education and Instructional Technologies

Supervisor: Assoc. Prof. Dr. Ömer Delialioğlu

September, 2014, 114 pages

The aim of the current study was to explore (i) the initial perceived knowledge and skill level of high school students, and teachers in IT security; (ii) the effect of a developed Security Portal (SP) on perceived knowledge and skill level of the high school students in IT security, and (iii) students' satisfaction with the SP. In line with the current study aims, descriptive research design and survey method was employed. As the data collection instrument, two different versions of the Perceived Knowledge and Skills in IT Security Questionnaire (PSKiITSQ) were developed and used. To measure the initial perceived knowledge and skill level in IT security, the first version of the survey (PSKiITSQ-1) was utilized. To understand the effect of the portal and student satisfaction with SP, the second version (PSKiITSQ-2) was administered to the high school students. In total, 263 complete responses were obtained from students and 22 from teachers for the PSKiITSQ-1; and 132 complete responses from students for the PSKiITSQ-2. Results of the survey indicated that significant majority of the students were neither well informed about IT security at school nor at home. Except three items,

which are (i) adding owner information to IT devices with Android OS, (ii) not opening e-mails from unknown senders, and (iii) security-privacy settings of SNSs, majority of the students rated their perceived knowledge and skill in IT security below “good” level. Similarly, except proper use of e-mail, teachers also rated their knowledge and skill in IT security below “good” level. Current study results indicated that SP had a positive effect on students’ knowledge and skills in IT security and this change was statistically significant. Great majority of the students were satisfied with SP.

Keywords: Information Technology Security, Security Portal (SP)

## ÖZ

### ÖĞRENCİLERİN BT GÜVENLİĞİ ALANINDAKİ BİLGİ VE BECERİ DÜZEYLERİNİN GELİŞTİRİLMESİNDE GÜVENLİK PORTALININ ETKİSİ

Pancar, Nilay

Yüksek Lisans, Bilgisayar ve Öğretim Teknolojileri Eğitimi Bölümü

Tez Yöneticisi: Doç. Dr. Ömer Delialioğlu

Eylül, 2014, 114 pages

Bu çalışmanın amacı, öğrencilerin ve öğretmenlerin (1) BT güvenliği hakkında hâlihazırda algıladıkları bilgi ve beceri seviyelerini, (2) Güvenlik Portalı'nın (GP) öğrencilerin BT güvenliğinde algıladıkları bilgi ve beceri seviyeleri üzerine etkisini ve (3) öğrencilerin GP ile ilgili memnuniyetini incelemektir. Çalışmanın amaçları doğrultusunda betimleyici araştırma tasarımı ve anket yöntemi kullanılmıştır.

Veri toplama aracı olarak BT Güvenliği Hakkında Alınan Bilgi ve Beceri Anketi (PSKiITSQ)'nin iki farklı sürümü hazırlanmış ve kullanılmıştır. Öğrencilerin ve öğretmenlerin BT güvenliği hakkında algıladıkları bilgi ve beceri giriş seviyelerini ölçmek için anketin ilk sürümü olan PSKiITSQ-1 kullanılmıştır. Güvenlik Portalının etkisini ve öğrencilerin GP memnuniyetini anlamak için anketin ikinci sürümü olan PSKiITSQ-2 lise öğrencilerine uygulanmıştır. Toplamda 263 öğrenci ve 22 öğretmen PSKiITSQ-1'i ve 132 öğrenci PSKiITSQ-2'yi tamamen cevaplamıştır. Anketin sonuçları göstermektedir ki, öğrencilerin kayda değer çoğunluğu ne okulda ne de evde BT güvenliği hakkında iyi bilgilendirilmemektedirler. Üç konu dışında, (i) Android

cihazlarına sahip bilgilerinin eklenmesi, (ii) bilinmeyen kişilerden gelen e-postaların açılmaması ve (iii) sosyal paylaşım sitelerinin güvenlik-gizlilik ayarları, öğrencilerin büyük çoğunluğu BT güvenliği hakkında hâlihazırdaki bilgi ve becerilerini “iyi” seviyenin altında değerlendirmişlerdir. Benzer biçimde e-postanın doğru kullanımı dışında öğretmenlerin de büyük çoğunluğu BT güvenliği hakkında hâlihazırdaki bilgi ve becerilerini “iyi” seviyenin altında değerlendirmişlerdir. Çalışmanın sonuçları GP’nın öğrencilerin BT güvenliği hakkındaki bilgi ve beceri seviyeleri üzerinde etkisi olduğunu ve bu değişimin istatistiksel olarak anlamlı olduğunu göstermektedir. Öğrencilerin büyük çoğunluğu GP’dan memnun kalmışlardır.

Anahtar Kelimeler: Bilişim Teknolojileri Güvenliği, Güvenlik Portalı GP



To My Family

## ACKNOWLEDGEMENTS

First and foremost, I would like to express my sincere gratitude to my supervisor Assoc. Prof. Dr. Ömer DELİALİOĞLU for his guidance, support, enthusiasm, valuable feedback and all the constructive conversations we had throughout the current study. Without his support and guidance, the current study would never have been accomplished. I would like to thank Dr. Recep Serkan ARIK, Nebahat İNCE, Berkan ÇELİK, and Ülkü OCAK for sparing their valuable time and supporting me on the current study. Furthermore, I would like to thank Nejat AKIN for his valuable support which started at the first days of my university life.

I would like to express my sincere appreciation to the examination committee members, Prof. Dr. ZahideYıldırım, Dr. Hasan Karaaslan, Assist. Prof. Dr. Cengiz Savaş Aşkun, and Assist. Prof. Dr. Halil Ersoy.

I would like to express my deepest gratitude to my family; to my parents Nasır and Leyla PANCAR who stood for us all their lives, to my dear brothers Nurettin and Nail PANCAR for their unlimited love, support, caring, and guidance. My dear family, your support has made me who I am today. I am proud to be a part of this family. I would like to extend my deepest appreciation to Ali ÇİFTÇİ, new member of our family and my love. Thank you all for your love, support, and being next to me when I needed you the most.

The study was supported by Middle East Technical University (METU)-Scientific Research Project Department.

## TABLE OF CONTENTS

|   |     |
|---|-----|
| ABSTRACT .....  | v   |
| ÖZ.....   | vii |
| ACKNOWLEDGEMENTS .....                                | x   |
| TABLE OF CONTENTS .....                               | xi  |
| LIST OF TABLES .....                                  | xiv |
| LIST OF FIGURES .....                                 | xv  |
| LIST OF ABBREVIATIONS .....                           | xvi |
| CHAPTERS .....  | 1   |
| 1. INTRODUCTION .....                                 | 1   |
| 1.1 Background of the Study .....                     | 3   |
| 1.2 Statement of the Problem.....                     | 6   |
| 1.3 Purpose of the Study.....                         | 7   |
| 1.4 Significance of the Study .....                   | 8   |
| 1.5 Research Questions .....                          | 10  |
| 1.6 Definitions of Terms .....                        | 11  |
| 2. LITERATURE REVIEW .....                            | 13  |
| 2.1 Computers in School .....                         | 14  |
| 2.2 Technology Integration into K-12.....             | 17  |
| 2.3 Threats Related to Kids & Protection Efforts..... | 18  |
| 2.4 IT Security Actions in Turkey .....               | 25  |
| 3. RESEARCH METHODOLOGY .....                         | 27  |
| 3.1 Research Design .....                             | 27  |
| 3.2 Research Questions .....                          | 27  |
| 3.3 Data Collection Instruments.....                  | 28  |

|          |  |    |
|----------|--|----|
| 3.3.1.   | Structure of the Perceived Knowledge and Skills in IT Security Questionnaire (PSKiITSQ) .....                                  | 28 |
| 3.3.1.1. | Perceived Skills and Knowledge in IT Security Questionnaire 1 (PSKiITSQ-1) .....   | 29 |
| 3.3.1.2. | Perceived Skills and Knowledge in IT Security Questionnaire 2 (PSKiITSQ-2) .....   | 30 |
| 3.3.2.   | Pilot Study .....  | 31 |
| 3.4.     | Implementation of the Perceived Knowledge and Skills in IT Security Questionnaire (PKSiITS) .....                              | 33 |
| 3.5.     | Data Analysis .....  | 34 |
| 3.6.     | Participants .....   | 34 |
| 3.7.     | Procedures .....   | 38 |
| 3.7.1.   | Context .....  | 38 |
| 3.7.2.   | Security Portal (SP) .....   | 39 |
| 3.7.2.1. | Analysis Phase of the SP .....   | 39 |
| 3.7.2.2. | Design and Development of the SP .....   | 40 |
| 3.7.2.3. | Coding of SP and Content Development .....   | 51 |
| 4.       | RESULTS .....  | 55 |
| 4.1.     | Demographic Information about the Participants .....   | 55 |
| 4.2.     | IT Security Rules and Being Informed .....   | 57 |
| 4.3.     | Study Results on Research Questions 1 and 2 .....  | 59 |
| 4.4.     | Study Results on Research Question 3 .....   | 66 |
| 4.5.     | Study Results on Research Question 4 .....   | 73 |
| 5.       | DISCUSSION AND RECOMMENDATIONS .....   | 75 |
| 5.1.     | IT Rules at School and at Home .....   | 75 |
| 5.2.     | Students' and Teachers' Initial Perceived Knowledge and Skill Level in IT Security (Refers to Research Question 1 and 2) ..... | 77 |
| 5.3.     | Effect of SP on Students' IT Security Knowledge and Skill Level (Refers to Research Question 3) .....                          | 78 |
| 5.4.     | Conclusion .....   | 80 |

|   |     |
|---|-----|
| 5.5. Limitation of the Study .....  | 80  |
| 5.6. Implications for Research .....  | 81  |
| 5.7. Suggestion for Further Research.....   | 81  |
| REFERENCES.....   | 83  |
| APPENDICES .....  | 91  |
| A. FINAL VERSION OF PKSOITS-1 (INTURKISH) .....   | 91  |
| B. FINAL VERSION OF PKSOITS-2 (INTURKISH) .....   | 99  |
| C. TABLE OF SPECIFICATION (TOS) (IN TURKISH).....   | 103 |
| D. APPROVAL WAS TAKEN FROM ETHICS COMMITTEE OF METU RESEARCH<br>CENTER FOR APPLIED ETHICS.....  | 107 |
| E. PERMISSION WAS TAKEN FROM MINISTRY OF TURKISH MINISTRY OF<br>NATIONAL EDUCATION (MONE) ..... | 109 |
| F. WILCOXON SIGNED RANKS TEST ANALYSIS RESULTS .....  | 111 |

## LIST OF TABLES

### TABLES

|  |     |
|--|-----|
| Table 3.1 Demographic data of the pilot study .....  | 32  |
| Table 3.2 Students' demographic data in the current study.....   | 36  |
| Table 3.3 Teachers' demographic data in the current study .....  | 37  |
| Table 3.4 Second level subtopics under "Let's get informed" and "Video/Animation ..  | 42  |
| Table 4.1 Initial characteristic of the students.....  | 56  |
| Table 4.2 Rules at school and at home about usage of IT devices .....  | 57  |
| Table 4.3 Teachers' initial perceived knowledge and skills in IT security .....  | 60  |
| Table 4.4 Students' Initial perceived knowledge and skills of in IT security .....   | 62  |
| Table 4.5 Students' perceived knowledge in virus infections results before and after SP<br>use .....   | 66  |
| Table 4.6 Students' perceived awareness about IT crimes and unlicensed products<br>results before and after SP use.....                        | 66  |
| Table 4.7 Students' perceived knowledge and skill level on common security settings of<br>OSs results before and after SP use.....             | 68  |
| Table 4.8 Students' perceived knowledge and skill level on security settings of Windows<br>OS results before and after SP use.....             | 69  |
| Table 4.9 Students' perceived knowledge and skill level on security settings of Android<br>OS results before and after SP use .....            | 70  |
| Table 4.10 Students' perceived knowledge and skill level on security settings of email<br>services results before and after SP use .....       | 71  |
| Table 4.11 Students' perceived knowledge and skill level on security settings of web<br>browsers and SNSs results before and after SP use..... | 72  |
| Table 4.12 Students' satisfaction level with SP.....   | 72  |
| Table C.1 Table of specification (TOS) (in Turkish) .....  | 103 |
| Table F.1 Wilcoxon signed ranks test analysis results.....   | 111 |

## LIST OF FIGURES

### FIGURES

|  |    |
|--|----|
| Figure 2.1 Percentage of students reporting that there is a computer available for them to use at home, school or other places (Source: OECD, 2005)..... | 15 |
| Figure 2.2 Access to computers at home or at school in PISA 2000 and PISE 2003 (Source: OECD, 2005).....   | 16 |
| Figure 2.3 Typology of risks (Source: OECD, 2012).....   | 19 |
| Figure 3.1 Blueprint of SP .....   | 41 |
| Figure 3.2 A screenshot login page of SP.....  | 43 |
| Figure 3.3 A screenshot Homepage of the SP.....  | 44 |
| Figure 3.4 Screenshot from <i>Let's Get Informed</i> menu .....  | 45 |
| Figure 3.5 Screenshot from article about SNSs' privacy settings.....   | 46 |
| Figure 3.6 Screenshot from video about screensaver settings of Windows .....   | 47 |
| Figure 3.7 Screenshot from published question and answers with explanations .....  | 48 |
| Figure 3.8 Screenshot from administration page .....   | 49 |
| Figure 4.1 Response percentages to questions about being informed about information security by school or parents.....                                   | 58 |
| Figure 4.2 Response percentages to questions about written IT rules at school .....  | 59 |

## LIST OF ABBREVIATIONS

|       |   |
|-------|---|
| ADDIE | Analyze, Design, Development, Implementation, and Evaluate    |
| FATİH | Enhancement Opportunities and Technology Improvement Movement |
| METU  | Middle East Technical University                              |
| MoNE  | Ministry of National Education                                |
| IT    | Information Technology  |
| OSs   | Operating Systems   |
| SNSs  | Social Network Sites  |
| SP    | Security Portal   |



## CHAPTER 1

### INTRODUCTION

*“Human factor is truly security’s weakest link.”*

*(Mitnick, Simon, & Wozniak, 2003, para. 7).*

Information has been an important asset of human beings for many years. With the broader use of Information Technology (IT) in commerce and daily life, information in some areas such as banking, communication, commerce, etc. has been transferred to the digital environment. As part of this technology dissemination, keeping information safe has become a major concern. This concern has increased sharply in parallel to the developments in IT. Storing and processing information in computers, and transferring it through computer networks becomes risky due to improper and/or incomplete security policies and malicious acts of users (Peng & Ramaiah, 2007). The concern about keeping information, computers and network systems safe and secure has created a new research and work area called IT security.

IT security can be defined as processing, saving, protecting, transmitting, and receiving information in a safe manner via computers and/or computer networks. There are four important terms which are mostly used in the area of IT security, which are threat, vulnerability, attack, and risk which can be explained as follows (Rufi, 2006; Delialioğlu, 2011):

- *Threat* is a circumstance or an event with the possibility to cause harm to the information or IT systems. Potential threats include (1) the human(s) factor which has a possibility to harm information or IT systems, (2) vulnerabilities of the IT systems formed either by hardware, software or human factor and (3) environmental factors. Main threats are social engineering, viruses, malware, bots, zombies, phishing messages, password sniffing, browser exploitation, social network profile exploitation, financial fraud, software vulnerabilities. Beside these online threats, there are also offline threats like shoulder surfing, dumpster diving, and laptop/mobile device theft which should be taken into consideration (Thompson, 2006; Hazari, Hargrave & Clenney. 2008; Mensch & Wilkie, 2011;).
- *Vulnerability* is the weakness in hardware, software or human factor that may cause any threat, risk or attack.
- *Attack* is “any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself.” (Committee on National Security Systems, 2010).
- *Risk* is the possibility of occurrence of a threat formed by any vulnerability.

Any type of vulnerability may open a door for attacks. Since IT companies work consistently on minimizing the vulnerabilities of their products, attackers focus more on the human factor which is called social engineering. For example, a software product may have authorization via a username and password and if the user gives his/her username and password to someone else or writes down this information somewhere or creates a weak password, authorization will not work as planned anymore. Another example is that software may have security settings but if the user turns off some features of these settings, the software might fail to protect the information. These examples indicate that the human factor might be the weakest and unknown link of the security chain. Therefore, increasing the knowledge and skills of the individuals about using IT products consciously is as important as the corporations' security programs and laws.

The most naive and curious IT users might be the students regarding their age and experience. It is known that especially students will have opportunities to use IT resources without supervision, their knowledge and skill level about IT security becomes more important than just restrictions to apply. Students' knowledge and skill about IT security could be increased by exposing them to the information about IT security (Bagchi-Sen et al., 2006). Teachers and parents are the most important people in young students' lives and their knowledge and skills in IT security could be crucial in keeping students safe. Training teachers and parents about IT security seems to be as important as training students since teachers and parents are one of the best sources to provide students with the information about IT security (Hentea, 2005). The usage of Internet resources, such as websites, forums, videos, interactive animations etc. could provide a new channel of information delivery to enhance the knowledge and skill level of students regarding IT security.

### **1.1 Background of the Study**

At present, IT is an important platform for education and research (Chou & Peng, 2010; Peng & Ramaiah, 2007). In addition to its benefits, the use of IT resources outside school increases concerns about the safety, privacy and abuse of children. Parents, educators, public health officials, and the media around the children have expressed an increased concern related to the security problems of IT products over the past decade (Jones, Mitchell, & Finkelhor, 2011; Valcke, Schellens, Van Keer, & Gerarts, 2007; Wishart, 2004). IT security vendors' reports, as listed below, indicate that threats are increasing from year to year and attackers focus more on vulnerabilities of related end users, such as humans' unconscious use of IT resources. Below are some important points from these reports:

1. IT Threat Evolution:Q2 2013 (Kaspersky, 2013):
  - a. A total of 983,051,408 threats have been detected in second quarter of 2013.

- b. These threats are 577,159,385 web-based attacks, 400,604,327 computer infections and 29,695 mobile malware.
2. Internet Security Threat Report (Symantec Corporation, 2013)
- a. Attackers use targeted attacks which mean that attackers collect information about the victim such as e-mail addresses, job, professional interests, attended conferences and visited websites.
  - b. Attackers use their tools to collect private information or control users IT devices such as logging keystrokes, viewing computer screens, and turning on computers' microphones and cameras.
  - c. Attackers may use web sites to add their codes to the victims' computer.

These findings show that threats and especially user related threats are increasing sharply; and IT security means not only internet security but also security of IT resources. One can use different security tools; however, some malicious codes may be new (zero-day threat), and security tools such as firewall or antivirus may not identify these malicious codes. Therefore, the knowledge and skills of each individual becomes even more important.

The Turkish Statistical Institute (TUİK) reports that computer and internet usage rate among 16 years old pupils is increasing every year (TUİK, 2012, 2013). In addition to personal usage of IT devices, there are large scale projects on the integration of technology into education in Turkish schools. Within the scope of these projects, technology enhanced classes with interactive boards, projectors and Wi-Fi access were established and students have been provided with free tablet computers by Turkish Ministry of National Education (MoNE). As part of the Bring Your Own Device (BYOD) movement, they also have the opportunity to use their own devices (computers, tablet pcs, mobile devices, etc.) in and out of school. The Turkish Ministry of National Education has a technical specification document called "Technical Specification for Computers to be used in IT Classes" which includes IT security solutions for hardware and software (MEB, 2011). According to this technical specification, computers should

have licensed software, updated anti-virus, a security card, and a lock for computer case (MEB, n.d.). In addition to the technical specification, a web filtering program administered by MoNE is used in IT classes.

Within the scope of the FATİH project, MoNE makes the contractor company to ensure that tablet computers have user limitations, management and security software as well as limited Internet connection out of the school area (MEB, 2011a). Furthermore, MoNE prepared *Conscious and Secure Usage of IT Tools* guidelines to increase the awareness about proper use of IT tools (MEB, n.d.). MoNE also issued a circular about *Internet Ethics* which includes information and rules on using the Internet properly (MEB, 2004). However, providing rules on the use of IT resources may not be enough to protect the students. According to a study carried out with IT teachers in Turkey, although there is web filtering and blocking as a security measure in IT classes, students find alternative ways to bypass this filter; one of the teachers who participated in the study stated that “...*filtering works effectively with Turkish and English words; however, German, French or Russian is not blocked. My students could access a Russian improper website...*” (Kabakçı & Can, 2009). Furthermore, students may use computers or tablets which do not have the protective tools or guidance. Just applying security infrastructure such as filtering monitoring, or anti-viruses may not be enough to protect students and information. In addition to a well-designed and implemented security policy document, raising students’ knowledge and skills about IT security will help keep themselves and their information safe.

For many countries, keeping students safe in online environment is a main concern; thus, they have developed different projects to increase knowledge and skills in using IT tools safely. Studies indicate that countries have governmental and nongovernmental projects to keep students safe. In some countries such as the USA, Norway, Hungary, Korea, Hong Kong, Greece, and Taiwan, governments support some projects to raise knowledge and skills of students, parents, and teachers in IT security (Hentea, 2005; Chou & Peng, 2011). Similarly, in some countries such as Belgium, France, Monaco,

and Switzerland schools appeal to nongovernmental associations to keep students safe (Wishart, 2004; Valcke, Schellens, Van Keer, & Gerarts, 2007).

## **1.2. Statement of the Problem**

Information is the most valuable asset not only for individuals, but also for organizations. Thanks to developing technology, information is transferred to the online environment. In addition to the business world, technology has become a part of the school environment as well. With the integration of technology into education, teachers use IT devices in a variety of ways and fields such as science, math, and English classes, or for social studies as a research or problem-solving/decision-making tool (Barron, Kemker, Harmes, & Kalaydjian, 2003). Students use IT devices for school activities such as doing homework, searching for a topic on the Internet, and communicating with teachers and their friends (Barron, Kemker, Harmes, & Kalaydjian, 2003; OECD 2012). Therefore, students have become more familiar with the IT devices and use them more than they did in the past.

Despite the benefits of technology, unconscious usage of IT may result in vulnerabilities, risks, threats or attacks. Symantec Corporation (2013) reported that attackers use targeted attacks, which means that attackers collect information about the victim such as their e-mail addresses, jobs, professional interests, conferences they attended, and websites they visited. IT security vendors' reports indicate that threats are increasing every year and attackers focus more on vulnerabilities related end users such as humans' unconscious use of IT resources (Kaspersky, 2013; Symantec Corporation, 2013). In addition to unconscious usage of the Internet, threats may occur via (i) installing programs which contain malicious codes (ii) lack of knowledge about the security settings of used operating system, security programs, packaged programs etc.

Bagchi-Senet et al. (2006) state that students behave more consciously if their environment behaves consciously about IT security. The school environment is important since it could help students develop the required skills about technology usage

and security (ETPRO-NCSA, 2012). However, schools might not focus enough on the security issues since published IT security standards or circulars are not a part of the curricula and they might not be assessed or accredited. Instead of taking supportive actions to raise students' knowledge and skills about safety and security, schools can have a tendency to solely just apply security devices and tools to monitor the students or prevent students to enter websites with malicious content (ETPRO-NCSA, 2008). In addition to schools' implementations, teachers' are the key stakeholder group to motivate and inform students on how to improve their knowledge and skills to use technology appropriately and ensure safety and security. According to the results of the studies carried out by ETPRO-NCSA with 1569 and 1003 educators in 2008 and 2010 respectively, as educators boost their confidence, they become more prepared to discuss security issues with their students.

Students' awareness level about creating strong passwords, online safe communication, scanning for malicious software, protecting information, personal computer security, managing firewalls, and filtering is at low level (Tekerek, 2012). Symantec reports, Turkish Statistical Institute reports, and study results carried out by Tekerek (2012) indicate that the importance of IT security increases every year. It is important to investigate how students' knowledge and skills in IT security can be improved. In order to improve students' knowledge and skills in IT security, to make them understand their responsibilities as citizens and help them use IT resources productively and effectively, students' knowledge and skills should be improved to distinguish the precise information and misinformation, to predict potential consequences of their actions in online environments, to notice the safety and security risk and threats, and to be able to prevent vulnerabilities (Lantzy, 2009).

### **1.3. Purpose of the Study**

The purpose of the current study was to measure students and teachers' existing perceived knowledge level and opinions about IT security design and to develop a

security portal to identify its effect on raising students' perceived knowledge and skills about security settings of IT resources. The literature was reviewed to examine the previous projects which were carried out to increase students' knowledge and skills about IT security. Regarding the projects done in different countries, in the current study a security portal supported by Middle East Technical University-Scientific Research Project was designed and developed. In accordance with the purpose of the study, a security portal was designed and examined to see how this portal affects the perceived knowledge and skills of students in using Information Technology (IT) resources securely. The mentioned security portal has separate interfaces for students, families, and teachers. Parents and teacher interfaces were designed for further research. It included information resources in different media forms such as articles, and videos related to IT security. Articles, videos, and forums were designed to investigate the impact of online materials on the perceived knowledge and skills. The portal includes vulnerabilities, current threats, risks and security settings of Social Networking Sites (SNSs), browsers, internet and popular Operating Systems (OSs) which are Windows, Android, and MAC OS. Parents' and teachers' content included additional information about parental controls, IT security resources for schools.

#### **1.4. Significance of the Study**

IT has numerous positive effects on education, such as ease of access to information, improved simulation capabilities, enhanced productivity, and means to provide technology-based assistive support (ETPRO-NCSA, 2008). On the other hand unconscious or inappropriate usage of IT may cause severe loss-of reputation, privacy or money. Supporting students to improve their knowledge and skills in IT security will help them protect themselves and ensure more safe and secure national infrastructure (ETPRO-NCSA, 2008).

In Turkey, all high school students, except for the ones studying in the “informatics department”, have only two elective courses related to IT, which are “information and



communication technology” and “project preparation”. “Information and communication technology” course has two textbooks with the same title as the course. These textbooks have almost the same content (Balaman, 2013; Eroğlu, & Yazar, 2013). The security part of the textbooks had information about information theft, using updated antivirus, turning on a firewall, back up, using password, viruses, virus types, information loss and copyright. Textbooks do not include information about how to set up and manage the security settings of IT resources. Briefly, in the textbooks, certain IT security issues were mentioned but how to ensure the security of IT resources was not mentioned. Thus, high school students may lack knowledge and skills about security settings of IT resources. In Turkey, students have limited awareness about issues related to rules and knowledge about security (Tekerek, 2012). Furthermore, instead of taking action to raise students’ knowledge and skills about safety and security, schools prefer to apply filters or use firewalls which block the websites (ETPRO-NCSA, 2008). However, the concern is that “when students leave school they need to know what behaviors are appropriate and effective, so they are prepared for IT environments with less protection, and can act responsibly” (ETPRO-NCSA, 2008). Furthermore, such protection methods may decrease the effectiveness of technology use at school. Therefore, filters or firewalls may block the websites that students need to use or may block some applications that students use to communicate with their teachers or classmates (Project Tomorrow, 2008).

There are also protection actions at the ministry level. MoNE prepared a required list for IT classes named “*Technical Specification for Computers to be used in IT Classes*” which includes IT security solutions for hardware and software used at IT classes (MEB, 2011a.). According to this technical specification, a computer should have licensed software, updated anti-virus, security card, and a lock for the case. In addition to the technical specifications, a web filtering program which is administered by the Ministry is used at the IT classes. The ministry also issued a circular about “Internet Ethic” which includes information and rules on using internet properly (MEB, 2004).

However, schools do not focus enough on the security issues since published IT security standards or circulars are not a part of the curricula and they are not assessed.

This study will contribute to the literature by examining the initial perceived knowledge and skills of students and teachers in IT security and the effect of an online support tool on students' perceived knowledge and skills in IT security. Analysis of the initial perceived knowledge and skills of students and teachers will provide information about the knowledge and skill level of the students and the teacher in IT security; and this information will help deciding if additional action should be taken to improve their knowledge and skills in IT security. The analysis of the effect of the online support tool on students' perceived knowledge and skills in IT security will provide significant evidence about the importance of such tools in students' knowledge and skills in IT security and how this tool can be integrated into students' life and education.

### **1.5. Research Questions**

The research questions guiding the current study are as follows:

1. What is the initial perceived knowledge and skill level of high school teachers in IT security?
2. What is the initial perceived knowledge and skills level of high school students in IT security?
3. Did using the security portal have a significant effect on the perceived knowledge and skill level of the students in IT security?
4. What is the satisfaction level of the students with the security portal?

## 1.6. Definitions of Terms

*Technology*: “Information technology such as computers, devices that can be attached to computers (e.g., LCD projector, interactive whiteboard, digital camera), networks (e.g., Internet, local networks), and computer software” (NCES, 2008).

*Information Technology (IT)*: “The technology involving the development, maintenance, and use of computer systems, software, and networks for the processing and distribution of data” (*Merriam-Webster's Collegiate Dictionary, n.d.*).

*IT Resources*: In the current study, IT resources refer to any tool, device, or software that is used to create, process, and deliver information.

*IT Safety*: In the current study, IT safety refers to the privacy, integrity, and efficiency of IT.

*Security*: “Protection against malicious attack by outsiders (and by insiders)” (Rufi, 2006).

*IT Security*: In the current study, IT security refers to being free from threats, vulnerabilities, risks, or cyber-attacks.

*Perceived knowledge and skill in IT security*: In the current study, perceived knowledge and skill refers to the level of knowledge and skill in IT Security that one feels related to the security settings of IT devices.

*Portal*: A portal is a web-site that brings information and resources together from many sources to many users in an effective way.

*Security Portal (SP)*: In the current study, security portal refers to a web-site designed and developed for the current study as a supplementary material to improve students', families', and teachers' knowledge and skills about IT security.

*Social Networking Sites (SNSs)*: “Online social networks for communities of people who share interests and activities or who are interested in exploring the interests and activities of others (e.g., Facebook, MySpace)” (NCES, 2008).

## **CHAPTER 2**

### **LITERATURE REVIEW**

Evaluation of technology and broader use of the Internet has made Information Technology (IT) an essential medium for learning; and it has also become an important platform for education and research (Chou & Peng, 2011; Peng & Ramaiah, 2007). Students who used IT tools at an earlier age might gain skills to use IT tools to access, compile, synthesis, and exchange information effectively. Therefore, successful integration of IT into education can have important effects on students' academic and future work life (OECD, 2005; Mueller, 2010). Beside advantages, unconscious usage of IT tools may create threats that may cause damage to the users or the system, such as “destruction/corruption/ theft or loss/disclosure of information, denial of use, elevation of privilege, illegal usage, huge financial, social, or/and emotional damages” (Rufi, 2006; Liang & Xue, 2009). IT security is an important component of IT applications, and it needs to be taken into consideration seriously (Rufi, 2006). Therefore, supporting students to gain knowledge and skills in IT security is as important as teaching them how to use IT tools effectively.

In this part, the relevant literature is reviewed and studies related to the integration of IT into education and schools, IT threats and security issues, and protection efforts to inform students about secure IT use are presented.

## **2.1. Computers in School**

Successful integration of computers into education can have important effects on students' academic and future work life (OECD, 2005; Mueller, 2010). Schools are the places that help students shape their academic life and future work life. The situation of schools in human life and the evolution of the computer technology makes the computers important and inevitable for schools (Hsiao, Tu, & Chung, 2012; Cullingford & Haq, 2009; OECD, 2005). Schools are not supposed to just use the technology, but to lead it as well.

There are two main concerns for schools: (i) teaching students how to use computers and (ii) using computer programs to deliver the curriculum (Cullingford & Haq, 2009; OECD, 2005). The first, teaching students how to use computers, helps them develop specific skills for their future academic and professional lives. Those who use computers in school “will have the advantage of being familiar with different media common to the modern workplace, and should be able to use these ICT skills to access, compile, synthesize and exchange information effectively” (OECD, 2005). On the other hand, if schools/teachers do not use computers in a proper way, students may recognize computers as an instrument to play games instead of learning instrument (Garavaglia, Garzia, & Petti, 2013). The second, using computers for learning environments, helps educators to develop educational resources, create new educational approaches and helps teachers to increase communication/interaction with students. It also supports students by enhancing collaboration and team work in problem-solving activities, and controlling/monitoring their own learning (Cullingford & Haq, 2009; OECD, 2005). These concerns and positive effects of computers make policy makers and educational authorities to integrate computers into schools (OECD, 2005).

As shown in Figure 2.1, in 18 countries, the use of computers at school is at least five percent higher than the use of computers at home (OECD, 2005).

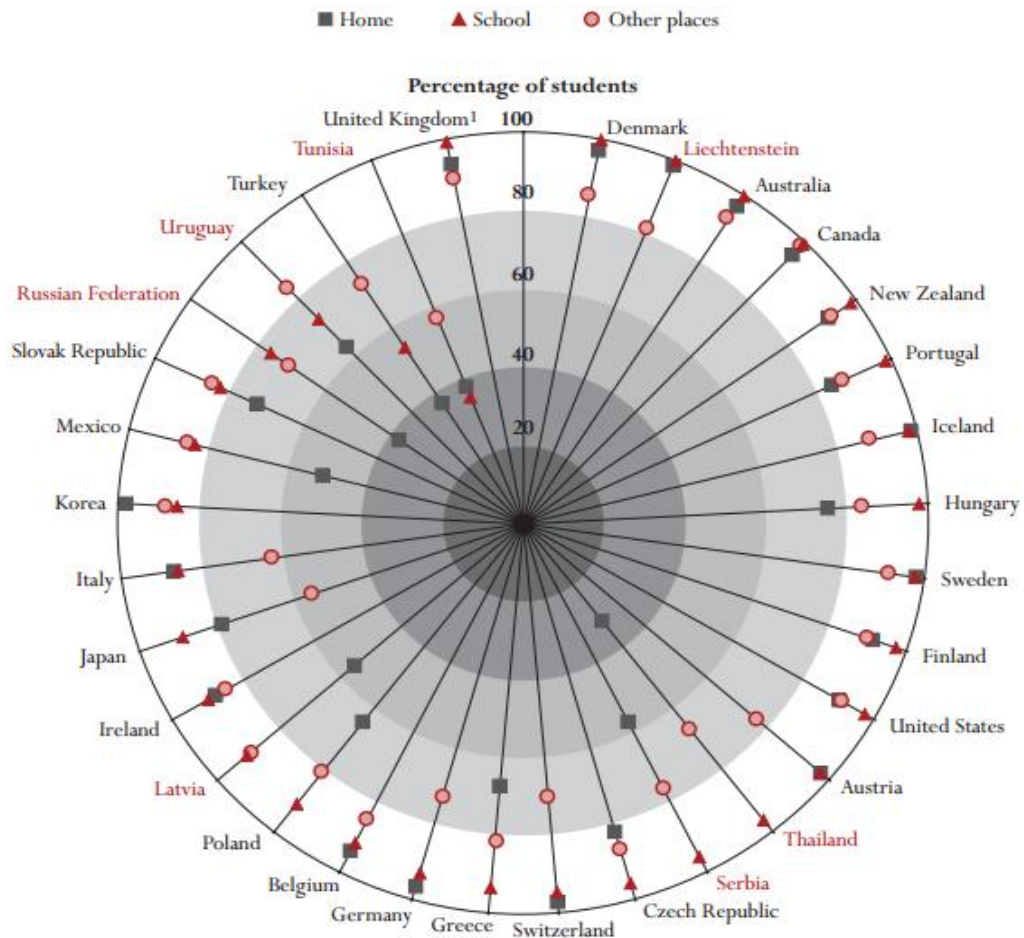


Figure 2.1 Percentage of students reporting that there is a computer available for them to use at home, school, or other places (Source: OECD, 2005)

As shown in Figure 2.2, access to computers at school and home rose significantly between 2000 and 2003 (OECD, 2005). In Turkey, the use of computers at school was below 60% in 2003 (OECD, 2005). As in other countries, there are projects to integrate technology into education in Turkish schools. Within the scope of *Enhancement Opportunities and Technology Improvement Movement (FATİH)*, which is the largest project on integrating technology into education in Turkey, approximately 732.500 tablet PCs were distributed to the students and 10.600.000 tablet PCs will be distributed (MoNE, 2013, 2014). Furthermore in 2011, 29.812 IT classes were established, and in 2013, the infrastructure of 38.000 schools was completed to ensure internet connection at schools (MoNE, 2013).

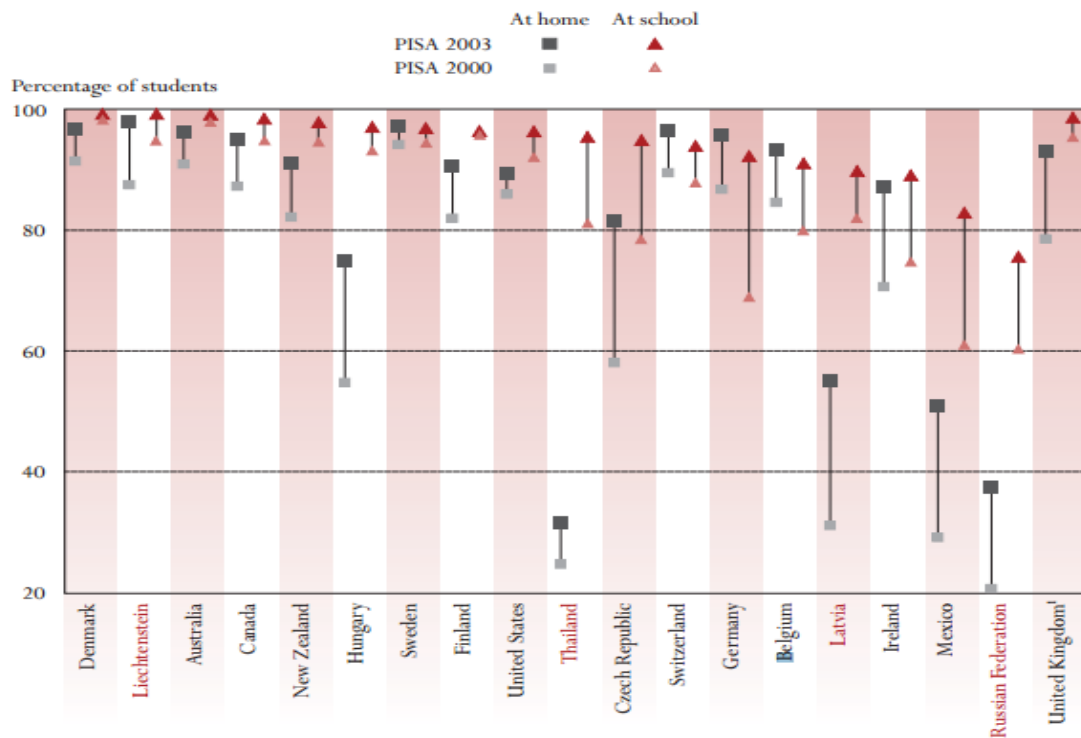


Figure 2.2 Access to computers at home or at school in PISA 2000 and PISA 2003 (Source: OECD, 2005)



## **2.2. Technology Integration into K-12**

Technology integration is defined as the use of technological devices, such as TVs, VCDs, projectors, desktop computers, laptops, handheld computers, software, or Internet in K-12 schools for instructional and educational purposes (Hew & Brush, 2007; Hechter & Vermette, 2013). In order to create better learning environments and to support students for their professional lives technology, integration into schools has increased rapidly (Snyder & Dillow, 2013; OECD, 2005). The International Society for Technology in Education (ISTE) published National Education Technology Standards for students “to learn effectively and live productively in an increasingly global and digital world”, for teachers “to teach, work and learn in an increasingly connected global and digital society”, and for administrators and leaders “to support digital age learning, implement technology and transform education landscape” (ISTE, n.d.).

At K-12 teachers’ technology use has increased in classrooms for instructional purposes and social studies as research or problem-solving/decision-making tool (Snyder & Dillow, 2013; Barron, Kemker, Harmes, & Kalaydjian, 2003). Studies have shown that technology integration influences students’ learning if it is used effectively by the teachers; and teachers’ technology skills are accepted as the most critical factor impacting technology integration into education (Hew & Brush, 2007; Inan & Lowther, 2010; Hechter & Vermette, 2013; Barron, Kemker, Harmes, & Kalaydjian, 2003). In teachers’ opinion, technology is an important component of teaching and learning, and teachers supported the use of technology in education. (An & Reigeluth, 2011). However, there are barriers to integrate the technology into K-12. These barriers are stated as resources, institution, subject culture, attitudes, beliefs, knowledge and skills, assessment, training, and support (Hew & Brush, 2007; An & Reigeluth, 2011; Hechter & Vermette, 2013).

### **2.3. Threats Related to Kids & Protection Efforts**

Evolution of information technologies offers unlimited opportunities to education, but it may also create potentially dangerous ideas. According to a study which examined online sites and prior studies about online risks and safer internet access, online risks that may affect children physically or mentally are adult content, pedophilia and sexual harassment, cyberbullying, offensive language, sexual discrimination or favoritism, online gaming and gambling, online violent games or images with violent representations, social disclosure, racism, bomb making or drug usage or gunfire usage, use of unreliable content, defamation, presentation of specific stereotypes, improper advertisements, and pirating (Lazarin, 2009). Livingstone et al. (2011) lists online risks as contact with people not known face to-face, offline meetings with online contacts, potentially harmful user-generated content and personal data misuse.

In addition to physical and mental risks, inappropriate usage of IT devices may result in financial losses. Threats that may result in losses are social engineering, viruses, malware, bots, zombies, phishing messages, password sniffing, browser exploitation, social network profile exploitation, financial fraud, software vulnerabilities. Beside these online threats, there are also offline threats like shoulder surfing, dumpster diving, and laptop/mobile device theft which should be taken into consideration (Mensch & Wilkie, 2011; Thompson, 2006; Hazari, Hargrave, & Clenney, B. 2008).

OECD (2012) categorizes the risks related children as shown in the Figure 2.3.

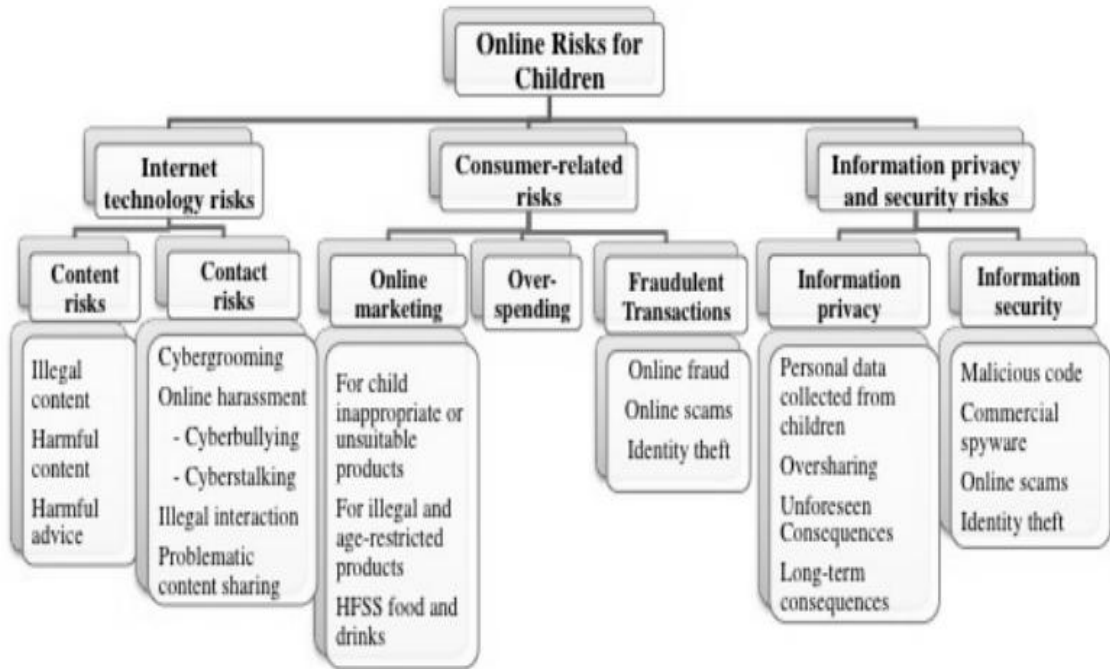


Figure 2.3 Typology of risks (Source: OECD, 2012)

A security chain is similar to a real chain and it is only as strong as its weakest link; and in IT security this link most of the time is the end user (Smith, 1998, Lieu, 2002; Mitnick, Simon, & Wozniak, 2003). In order to use IT devices safely, society needs to be get informed about IT security and its proper usage. This aim can be reached by a knowledgeable society and it is possible by raising knowledgeable members. With the integration of computers into education such as researching for homework, preparing e-portfolios, and using learning management systems, students use IT devices more often than before (Snyder & Dillow, 2013; National Cyber Security Alliance, 2014). Students also use these technologies in their daily lives such as searching information, playing

games, communicating with friends, finding new friends, and sharing ideas etc. (Livingstone et al., 2011; Tekerek 2012). Although using IT tools outside the school context is supported, there is a great concern over students' safety (Wishart, 2004). Raising students' awareness of the importance of Information Security plays a critical role in their Information Security Behavior. Exposing students to Information Security issues through schools, parents, and media is important to motivate their information security behaviors (Bagchi-Senet al., 2006). There are several security programs available for end users, such as authentication, firewall, anti-virus, anti-spyware, and browser-based tools (Mensch & Wilkie, 2011). The important issue is to know how to use these security programs. According to the results of a survey conducted in the scope of National Cyber Security Awareness Month (NCSAM), 70% of teen internet users have asked for or sought out advice on managing their privacy (National Cyber Security Alliance, 2014).

The responsibility of teaching students how to use IT tools safely and securely is a controversial issue. Results of a survey which was conducted by the National Cyber Security Alliance and Norton by Symantec (2010) with 3500 participants revealed that 90 % of the participants think that parents are responsible for teaching children to use computers safely and securely while 7% of them think teachers/schools are responsible for teaching children to use computers safely and securely. ETPRO-NCSA (2010) reports that 72% of teachers and 58% of technology coordinators think that parents are primarily responsible for teaching children to use computers safely and securely while 51% of school administrators think primarily teachers/schools are responsible for teaching children to use computers safely and securely. Findings of a study conducted by Hsiao, Tua and Chung (2012) indicate that perceived family support has a significant impact on computer self-efficacy; and computer self-efficacy has significant impact on computer use. On the other hand, some researchers claim that schools play a fundamental role in ensuring students' safety in the online environment (Wishard, 2004; Valcke, Schellens, Van Keer, & Gerarts, 2007; Livingstone, Haddon, Görzig, & Ólafsson, 2011). Livingstone et al. (2011) claim that schools have an opportunity to

reach all students in the learning environment with up-to-date technology and resources; thus, to gain digital literacy and safety skills, schools are supposed to support students and parents; parents also prefer to get information from their child's school (Livingstone et al., 2011). To protect students and provide better training, teachers need to know how to handle IT security issues and how to use computers (Hentea, 2005). Teicher (1999) states that managing online experience, knowing how to deal with uncomfortable and inappropriate information, and knowing when to seek adult help are the concepts that students must know. However, even if schools are expected to be responsible for students' safety and for their Internet-related teaching content; teachers themselves may lack adequate understanding of students' risky, unsafe, or unethical internet behaviors (Chou & Peng, 2011).

Schools provide internet safety via a restricted online environment (ETPRO-NCSA, 2008). However, even if web sites may have a reliable web address and seemingly reliable information, they may contain harmful information such as insulting jokes, offensive language, violent images, and improper materials (Lazarinis, 2010). Lazarinis (2010) also analyzed the log files of two schools within scope of his/her study and concluded that even if the security policies are operating, they may fail to block webpages with unreliable content and "students may be able to bypass the applied restrictions to visit their preferred sites." Therefore, although schools have security policies, they cannot completely prevent access to unreliable content.

In addition to school computers, students may use unsupervised and unfiltered IT devices at home. If students do not have sufficient knowledge and awareness level of IT security, their use may cause serious physical, mental, and financial problems (Wishart, 2004; Lazariniz, 2009; Mensch & Wilkie, 2011; Thompson, 2006; Hazari, Hargrave, & Clenney, B. 2008). Studies indicate that there is a high level of Internet use at home and little of this use is filtered or supervised by parents (Atkinson & Finn, 2009; Valcke et al, 2010; Livingstone et al., 2011). Control of IT security at home can be ensured with parental controls and firewalls; however, a degree of technical knowledge is needed to

install and use these security controls (Davidson & Martellozzo, 2008). Since most of the studies or projects are on raising awareness related to internet security, teachers and parents may have problems finding technical information about IT devices and software.

Lazarinis (2010) indicates that being aware of the problems related to IT security is important and specialized education programs need to be implemented for both parents and children to make them aware of these problems. The OECD prepared “Guidelines for the Security of Information Systems and Networks (“Security Guidelines”)” and released the “Implementation Plan for the OECD: “Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security” (“OECD Implementation Plan”)” in January 2003 to improve the “Culture of Security” among all participants who develop, own, provide, manage, service, and use information systems and networks (OECD, 2004). According to the “OECD Implementation Plan”, governments, businesses and civil societies are responsible from improving the “Culture of Security”. The findings of the survey based on the “OECD Implementation Plan” indicate that all responding (22 member countries) countries have developed a national policy for the security of information systems and networks or for those who are in the process of developing one. Except for one, all respondents worked on awareness raising, education, and training. Respondents circulate the “Security Guidelines” via different means such as hardcopies, electronic copies, and links to the OECD web site or files on national web sites (OECD, 2004). Respondents also carried out different implementations or projects to support “Culture of Security”: workshops, seminars, training, conferences, and associated papers and studies were conducted by Australia, the Czech Republic, France, Germany, Hungary, Japan, Korea, Mexico, the Netherlands, Portugal, and the US; *Web site(s) and portal(s)* were developed by Australia, Finland, France, Germany, Japan, Korea, the Netherlands, Portugal, Spain, Sweden, UK, and the US; Germany launched a targeted website for young people; the Netherlands sponsored a special issue of the “Donald Duck” cartoon magazine on safe Internet usage. Korea launched a Slogan/Poster Contest for elementary/middle/high school students on the

security of information systems and networks; and Norway prepared educational packages for elementary and middle schools (OECD, 2004).

Pittsylvania County Schools took some proactive actions to educate employees, students, and community stakeholders with respect to their choices relative to their use of the Internet. To this purpose, “Computer Technology Acceptable Use and Internet Safety Policy” was printed as a part of the Student Policy Handbook and distributed to all students. Schools requested parents and students to sign and return an acknowledgement of the receipt of these policies. At the beginning of the academic year, students also had to review this policy before using technology labs. Contents related to safety awareness and security settings were included in the students’ progress reports and in the Information Department’s newsletter during the academic year. Furthermore, guiding students began in kindergarten and continued through 12<sup>th</sup> grade; and guiding takes place during in-classroom instruction. Educators should also acknowledge “Computer Technology Acceptable Use and Internet Safety Policy” prior to their login to a computer at school. These efforts made 75% of instructors share Internet safety tips during class (McDaniel, & Early, 2013).

In 2000, the USA enacted the Children’s Internet Protection Act (CIPA), which requires schools and libraries that receive federal funds for discounted telecommunications, Internet access, or internal connections services to adopt an Internet safety policy and employ technological protections that block or filter certain visual depictions deemed obscene, pornographic, or harmful to minors. The Department of Commerce’s National Telecommunications and Information Administration (NTIA) was also assigned to evaluate if the current technology was suitable to meet the needs of educational institutions, and development and effectiveness of local Internet safety policies. In the scope of CIPA, NTIA identified best practices to use in developing Internet safety policies, and emphasized that the language of the legislature is important and it has to ensure that technology protection measures include more than just blocking and filtering technology (Victory, 2003). The National Institute of Standards and Technology (NIST)

also published “Building an Information Technology Security Awareness and Training Program: Computer Security” guideline to build and maintain a comprehensive awareness and training program, which included awareness and training program designs and implementation steps, as part of an organization’s IT security program (Wilson & Hash, 2003).

The U.S. Department of Homeland Security and the National Cyber Security Alliance has also organized an event every October called the National Cyber Security Awareness Month (NCSAM) for over a decade. This event is structured for four weeks targeting consumers, small and medium-size businesses, corporations, educational institutions, and young people across the nation. The organization that supports the event claims that every individual has a responsibility in securing the internet, and fulfilling the responsibilities is important for digital society (National Cyber Security Alliance, n.d.). Within the scope of the NCSAM, a survey was carried with 1,000 adults in the US aged between 18 and 26 to understand the online behaviors, attitudes and career aspirations of participants (Raytheon, 2013). Findings of the survey indicated that 82% of the participants used a password, 23% of the participants shared an online password with a non-family member, 66% of them connected to a no-password-required public WiFi; 30% of the participants met someone online, and 86% of the participants thought increasing cyber security awareness programs in a formal education program was important (Raytheon, 2013). The Washington State Coalition against Domestic Violence, Washington Violence against Women Network, and 18 Domestic violence agencies carried out a project called Technology Safety Project of the Washington State Coalition Against Domestic Violence about computer, internet safety, and stalking. The project was called “train the trainer” and the materials consisted of PowerPoint, handouts, and guidance. Even if the project seemed to involve adults, 75% of the participants had children so this project also affected children (Atkinson & Finn, 2009).

Taiwan Ministry of Education initiated Teacher Awareness of Internet Safety (TAIS), a 10 years project focused on internet safety for elementary and middle school teachers.



Of the core areas of the project, (1) “communication security and safety” referred to teaching students how to protect themselves from viruses, hackers, spam (junk mail), and illegitimate commercial transactions, and how to safeguard their confidential information, (2) “information decency and appropriateness” referred to identify malicious rumors, pornography, sexual solicitation, misleading advertising and ethical use of digital information, (3) “online interpersonal safety” referred to social interactions, and (4) “using computer/internet safely” referred to proper equipment, good working environment, eyesight protection, and posture. Within the project, a website called eteacher (<http://www.eteacher.edu.tw>) was designed with textual information, related links, research reports, forum, and chat room. Workshops, training programs, and conferences were also held to support the teachers. Results of the study carried out by Chou & Peng (2011) indicate that majority of the teachers (67.41%) used eteacher materials in their teaching practices, and materials on eteacher positively changed students’ knowledge, attitudes, and behaviors regarding their Internet usage.

#### **2.4. IT Security Actions in Turkey**

Since the use of computer and internet has increased sharply in the community and education, Turkish government has released guidelines and supported awareness raising programs. MoNE has prepared a required list for IT classes called “*Technical Specification for Computers to be used in IT Classes*” which includes IT security solutions for hardware and software (MEB, 2011a). According to this technical specification, computers in IT classes should have licensed software, updated anti-virus, security card, and lock for the case. In addition to the technical specification, a web filtering program that is administered by the Ministry is used in the IT classes and school networks. The Ministry has also issued a circular called “Internet Ethics” which includes information and rules on proper internet use for school administrators, teachers, and students (MEB, 2004). MoNE also published a booklet called “Recommendations for Secure Usage of the Internet” and distributed it to all primary school students and

teachers in 2009-2010 academic year. The booklet was also published online ([http://www.guvenliweb.org.tr/e\\_kilavuz/](http://www.guvenliweb.org.tr/e_kilavuz/)) (Presidency of Telecommunication, n.d.).

In accordance with Law No 5651 (2007), websites with inappropriate content are blocked to all citizens by Internet Service Provider (ISP). According to “Procedures and Principles Regarding the Safe Internet Service” enacted by the Information and Communication Technologies Authority (2011), ISPs in Turkey must provide free Secure Internet Service to citizens. Internet Service Providers (ISPs) must provide families with two user profiles, which are family and child profile. While a family profile is a normal user profile, a child profile is filtered according to data taken from the Information and Communication Technologies Authority. Information and Communication Technologies Authority also developed two websites: One of them is (<http://www.guvenlinet.org>) to guide families about using Secure Internet Services and the other (<http://www.guvenliweb.org.tr/>) is about using internet safely. The latter website includes information about internet security for families and educators. The Presidency of Telecommunication gives support to a website (<http://www.guvenlicocuk.org.tr>) which includes games and information about internet security.

In Turkey, all high school students except for the ones studying in the “informatics department” have only two elective courses related to IT which are “information and communication technology” and “project preparation”. The “Information and communication technology” course has two textbooks that carry the same title as the course. Content of the two textbooks is almost identical (Balaman, 2013; Eroğlu, & Yazar, 2013). The security part of the textbooks contains information about information theft, using updated antivirus, turning on a firewall, back up, using password, viruses, virus types, information lost and copyright. The textbooks do not include information about how to set up and manage security settings of IT resources. Briefly, in the textbooks, certain IT security issues are mentioned but how to ensure the security of IT resources is was not addressed.

## CHAPTER 3

### RESEARCH METHODOLOGY

#### 3.1. Research Design

The study followed a descriptive research design and survey method with statistical treatments. Descriptive statistics, such as frequency distributions, means, and standard deviations, were utilized to analyze students' initial perceived knowledge and skills in IT security. The Wilcoxon signed-rank test was also conducted to determine whether there was a significant change in the students' perceived knowledge and skills in IT security.

#### 3.2. Research Questions

The purpose of this study was to investigate (i) the initial perceived knowledge and skill level of the students and teachers in IT security, (ii) the effect of the Security Portal (SP) on students' perceived knowledge and skill level in IT security, and (iii) the students' satisfaction with using SP. The target groups of this research were Turkish high school students and their teachers. The research questions that guided the current study are listed below:

1. What is the initial perceived knowledge and skill level of high school teachers in IT security?
2. What is the initial perceived knowledge and skills level of high school students in IT security?

3. Did using the security portal have a significant effect on the perceived knowledge and skill level of the students in IT security?
4. What is the satisfaction level of the students with the security portal?

### **3.3. Data Collection Instruments**

The data were collected from the participants through two versions of a questionnaire called the Perceived Knowledge and Skills in IT Security (PSKiITSQ) (see Appendices A-B). The questionnaires were administered to 263 high school students in two different public high schools.

#### **3.3.1. Structure of the Perceived Knowledge and Skills in IT Security Questionnaire (PSKiITSQ)**

*“Tests are instruments or tools used to measure change. If the instrument itself is faulty, it cannot accurately measure changes in knowledge. A valid and reliable pretest and posttest must be made up of well-written and clear questions”* (I-TECH , 2010, p. 2).

In accordance with the definition to create a valid and reliable pretest and posttest, I-TECH guidance (2010) was used, which suggests to:

- Create questions that focus on the primary course objectives.
- Only include questions to which there are clear answers provided during the course.
- Develop a test that will take between 10-25 minutes to complete. (p. 2).

In order to include all main objectives of the study and to avoid non-related objectives, a table of specification (ToS) was developed. Items of the questionnaire were developed in line with the ToS items.

To ensure the validity, appropriateness, and comprehensibility of the questionnaires, two content experts, two statisticians, and two high school teachers evaluated PSKiITSQ

Content experts reviewed the questions in terms of the content appropriateness, statisticians reviewed the structure of the questions and questionnaires in terms of appropriateness for data analysis. High school teachers reviewed the questions in terms of comprehensibility and students' perceptions. Reliability Coefficient (Cronbach's alpha) in the questionnaire of the current study was 0.863. Cronbach's alpha,  $\alpha$ , value indicated that the test had good reliability (Field, 2006). The duration of the test was 15 minutes, which can be considered as the optimal duration. In order to make participants feel comfortable and provide honest answers, participants were asked to write down their self-created usernames. These usernames were used by the participants to login to the SP. These usernames were also used to match PSKiITSQ-1's and PSKiITSQ-2's data.

Two different versions of the Perceived Skills and Knowledge in IT Security Questionnaire (PSKiITSQ) were designed and administered. Questionnaires involved multiple choice, Likert type, and open-ended type questions.

### **3.3.1.1. Perceived Skills and Knowledge in IT Security Questionnaire 1 (PSKiITSQ-1)**

PSKiITSQ-1 is the first version of the PSKiITSQ, which includes questions about demographic information and perceived knowledge and skills in IT security. PSKiITSQ-1 was administered to the students and teachers before SP was introduced. Schools and teachers were supposed to support students and parents about IT security; however, teachers themselves may lack adequate understanding of students' risky, unsafe, or unethical internet behaviors (Livingstone et al., 2011; Chou, & Peng, 2011). To measure teachers' initial knowledge and skill level in IT security, PSKiITSQ-1 was also

administered to the teachers. To allow for a detailed analysis, the questionnaire was divided into eight subparts (Appendix A):

- General questions + demographic questions (9 questions)
- Initial knowledge about virus infection, protection programs, unlicensed products and being informed by school and parents (11 questions)
- Being informed about written IT security rules at schools (4 questions)
- Common security setting of OS (4 questions)
- Security settings of Windows OS (2 questions)
- Security settings of MAC OS (5 questions)
- Security settings of Android OS (3 questions)
- Security settings of e-mail (4 questions).
- Security settings of browsers and SNSs (3 questions).

PSKiITSQ-1 includes 45 questions. Participants rated their level of knowledge and skills on a 5-point Likert scale; 1 = Not at all, 2 = A little, 3 = Average, 4 = Good, 5 = Very good. PSKiITSQ-1 was also adapted for the teachers in order to examine their initial perceived knowledge and skills in IT security.

### **3.3.1.2. Perceived Skills and Knowledge in IT Security Questionnaire 2 (PSKiITSQ-2)**

PSKiITSQ-2 is the second version of the PSKiITSQ, which includes questions about perceived knowledge and skill in IT security and students' satisfaction with SP; and does not include questions related to demographic information. PSKiITSQ-2 was administered to the students after they used SP. PSKiITSQ-2 has the same structure as PSKiITSQ-1. In addition to the PSKiITS-1 questions, PSKiITS-2 included user satisfaction questions (Appendix B):

- General questions (2 questions)

- Knowledge about virus infection, protection programs, unlicensed products (6 questions)
- Common security setting of OS (4 questions)
- Security settings of Windows OS (2 questions)
- Security settings of MAC OS (5 questions)
- Security settings of Android OS (3 questions)
- Security settings of e-mail (4 questions).
- Security settings of browsers and SNSs (3 questions).
- User Satisfaction (16 questions).

User satisfaction questions were adapted from the study conducted by Yiğit, Yıldırım and Özden (2000). User satisfaction was measured by: (i) ease of finding information on the SP, (ii) appropriateness and comprehensibility of the content on the SP, (iii) usefulness of SP, and (iv) performance of SP (Sørum, Andersen, & Vatrapu, 2012). The alpha value indicated that the user satisfaction questionnaire have good reliability (Field, 2006). PSKiITSQ-2 also includes 45 questions. Participants rated their level of knowledge and skills on a 5-point Likert scale; 1 = Not at all, 2 = A little, 3 = Average, 4 = Good, 5 = Very good.

### **3.3.2. Pilot Study**

A pilot study of the questionnaire was conducted to determine if the items of the questionnaire were understood by the participants in the sample (Creswell, 2012; Van Teijlingen et. al., 2001). The pilot study survey included the questions revised based on feedback of the participants who completed and evaluated the questionnaire (Creswell, 2012). Procedures given in the study of Teijlingen & Hundley (2001) were followed to improve the internal validity of the questionnaire:

- administering the questionnaire to pilot subjects in exactly the same way as it will be administered in the main study

- asking the subjects for feedback to identify ambiguities and difficult questions
- recording the time taken to complete the questionnaire and decide whether it is reasonable
- discarding all unnecessary, difficult, or ambiguous questions
- assessing whether each question gives an adequate range of responses
- establishing that replies can be interpreted in terms of the information that is required
- checking that all questions are answered
- re-wording or re-scaling any questions that are not answered as expected
- shortening and revising

The pilot study was carried out at an Anatolian teacher high school with 145 students. Demographic data about the pilot study participants are shown in Table 3.1.

Table 3.1 Demographic data of the pilot study participants

| Grade      | <i>n</i>    |               | Total |
|------------|-------------|---------------|-------|
|            | <i>Male</i> | <i>Female</i> |       |
| 9th Grade  | 33          | 12            | 45    |
| 10th Grade | 3           | 3             | 6     |
| 11th Grade | 24          | 12            | 36    |
| 12th Grade | 29          | 29            | 58    |
| Total      | 89          | 56            | 145   |

Participants were requested to complete the questionnaire, and to write down their comments about questions if they had any (Creswell, 2012; Van Teijlingen & Hundley, 2001). There were different comments about the administered questionnaire. First of all,



the questionnaire consisted of 65 questions, and therefore the length of the questionnaire was the main problem. Hence, questions that were not directly related to security settings were excluded from the final version. Excluded questions are shown in italics in the questionnaire in Appendix A. In addition to the exclusions, five questions were added to the questionnaire. The first question added to the questionnaire was about which OS is used by the participants. This item was added to determine whether skipped items related to OSs settings were meaningfully and purposely skipped by the participant or not. Two of the questions were about security settings of Android OS, and the last two questions were about security settings of e-mail. Revisions were made on:

- Q15: Participants requested an “I do not know” choice. It was added to the questionnaire.
- The Likert type questions with “no comment” degree were changed with “average”.

The final version of the PSKiITSQ-1 was checked by two statistics experts. In line with the suggestions: (i) instead of the “*If you do not use MAC OS X please skip questions between 31-35*” direction, “*If you do not use MAC OS X please move to Section 6*” was used; (ii) instead of providing age intervals to obtain age data, the question was designed as an open-ended question.

#### **3.4. Implementation of the Perceived Knowledge and Skills in IT Security Questionnaire (PKSiITS)**

In order to administer the questionnaire, an approval from the Ethics Committee of METU Research Center for Applied Ethics (see Appendix D) and official permission from Republic of Turkish Ministry of National Education (MoNE) (see Appendix E) were obtained. Before distributing the PKSoITS-1, the researcher introduced herself and explained the aim of the study to the students. After this explanation, PKSoITS-1 was distributed to the students with a piece of paper which included the web address of the

SP ([www.bilinlibirey.com](http://www.bilinlibirey.com)). Students were reminded two or three times to write down a username that would be required to login to the SP. After PSKiITSQ-1 was administered, participants were informed that they could login to the SP starting from the next day. One week after the PSKiITSQ-1 administration, the researcher went to the schools and reminded students about the web address of the SP and their usernames. After three weeks of PKSoITS-1 administration, PKSoITS-2 was administered to the students. Students were reminded to provide the same username which they used to login to the SP on the distributed PSKiITSQ-2.

### **3.5. Data Analysis**

Collected data were analyzed by using the Statistical Package for the Social Sciences (SPSS 20). Descriptive statistics, such as frequency distributions, means, and standard deviations were used to analyze students' and teachers' initial perceived knowledge and skills in IT security. Since data were ordinal in the current study, the Wilcoxon signed-rank test was also performed to determine whether the changes in the students' perceived knowledge and skills in IT security were statistically significant (Hinkle, Wiersma, & Jurs, 2003) or not.

### **3.6. Participants**

The participants of the current study were high school students, and teachers. The current study was carried out in two different public schools. PSKiITSQ-1 was applied to 263 high school students and PSKiITSQ-2 was applied to 132 high school students who participated in PSKiITSQ-1 and used SP (Table 3.2). The age range of the participants was 14-19. All participants used at least one IT device. Students who participated in the current study took only one elective course about IT, which was "information and communication technology".

Schools were selected from different socio-economic areas. Demographic data of the students who filled in PSKiITSQ-1 shows that the socio-economic status of the students in the first school was between low to medium and in the second between medium to high. As shown in the Table 3.2, 111 (41.9%) of the 263 participants were from the school with students of low to medium socio-economic status and 152 (57.4%) of the 263 participants were from the school with students of medium to high socio-economic status. Of the 263 participants, 107 (40.7%) were female and 156 (59.3%) male. Of the 263 participants, 51 (19.2%) were in 9<sup>th</sup> grade, 74 (27.9%) in 10<sup>th</sup> grade, 79 (29.8%) in 11<sup>th</sup> grade, and 59 (22.3%) in 12<sup>th</sup> grade. The grade data of 2 participants were missing.

The socio-economic status of the students who voluntarily used the SP and filled PSKiITSQ-2 was as follows: of the 132 participants, 67 (50.8%) were from the school with students of low to medium socio-economic status and 65 (49.2%) were from the school between medium to high socio-economic status. Of the 132 SP using participants, 47 (35.6%) were female and 85 (64.4%) were male. Of these 132 participants, 30 (22.7%) were in 9<sup>th</sup> grade, 25 (18.9%) in 10<sup>th</sup> grade, 50 (37.9%) in 11<sup>th</sup> grade, and 27 (20.5%) in 12<sup>th</sup> grade.

Table 3.2 Students' demographic data in the current study

|                                | <i>f</i>    |            |
|--------------------------------|-------------|------------|
|                                | PSKiITS-1   | PSKiITS-2  |
| <b>Socio Economic Status</b>   |             |            |
| First school (low to medium)   | 111 (41.9%) | 67 (50.8%) |
| Second school (medium to high) | 152 (57.4%) | 65 (49.2%) |
| Total                          | 263         | 132        |
| <b>Gender</b>                  |             |            |
| Female                         | 107 (40.7%) | 47 (35.6%) |
| Male                           | 156 (59.3%) | 85 (64.4%) |
| Total                          | 263         | 132        |
| <b>Grade</b>                   |             |            |
| 9th grade                      | 51 (19.2%)  | 30 (22.7%) |
| 10th grade                     | 74 (27.9%)  | 25 (18.9%) |
| 11th grade                     | 79 (29.8%)  | 50 (37.9%) |
| 12th grade                     | 59 (22.3%)  | 27 (20.5%) |
| Total                          | 263         | 132        |

Teachers' data were used to answer the first research question. Of the teachers, 17 (77.3%) were female and 5 (22.7%) were male (see Table 3.3). The age range of the teachers was 29 - 56. Teachers' field of study was as given in Table 3.3.

Table 3.3 Teachers' demographic data in the current study

|                                     | <i>n</i> |
|-------------------------------------|----------|
| <b>Gender</b>                       |          |
| Female                              | 17       |
| Male                                | 5        |
| Total                               | 22       |
| <b>Teachers' field of the study</b> |          |
| Biology                             | 2        |
| Biomedical Device Technology        | 3        |
| Chemical                            | 1        |
| Electronic                          | 2        |
| English                             | 2        |
| Geography                           | 2        |
| History                             | 2        |
| Painting                            | 1        |
| Physics                             | 2        |
| Philosophy                          | 1        |
| Psychological Counsel               | 2        |
| Turkish Language and Literature     | 2        |

### **3.7. Procedures**

After the development of the SP, two public schools enrolled in the FATİH project were selected for data collection. Data collection procedure took three weeks. The schools were visited three times and the researcher attended classes to apply the PSKiITSQ. The first visit was to apply the PSKiITSQ-1. In the first visit, the aim of the study was explained to the students and they were asked to participate in the study. Then, students were distributed PSKiITSQ-1. In the second visit, which was one week after the administration of the PSKiITSQ-1, students were reminded about the SP and about their authentication information to login to SP. In the last visit, three weeks after the first visit, students were asked to complete the PSKiITSQ-2.

#### **3.7.1. Context**

The participants of the current study were Turkish high school students and teachers. For the current study, three public schools were selected; an Anatolian teacher high school, a technical and industrial vocational high school, and an Anatolian high school in the capital city of Turkey, Ankara. Schools were selected from districts of different socioeconomic level. The Anatolian teacher high school was a boarding high school and there were students from a wide range of socioeconomic status. The pilot study was conducted at this school to improve the internal validity of the questionnaire (Teijlingen & Hundley, 2011). Students were asked to complete the questionnaire and provide comments about the items. The main study was conducted at the Anatolian high school and the biomedical device technologies department of the technical and industrial vocational high school. The questionnaires were administered 9<sup>th</sup>, 10<sup>th</sup>, 11<sup>th</sup> and 12<sup>th</sup> grade students.

### **3.7.2. Security Portal (SP)**

Security portal is a web-site designed and developed for the current study as a supplementary material to support students' to improve their knowledge and skills in IT security. In order to design and develop SP, the first three phases of ADDIE as an instructional design model were utilized.

#### **3.7.2.1. Analysis Phase of the SP**

The main aim of the analysis phase was to analyze the target group and to set the objectives (Petarson, 2003). The target groups of the study were high school students. The main questions about the target group were "*What are the students' current resources about IT security?*", and "*What do they need to know?*"

Students' current resources about IT security were analyzed online since the common resources for the students were assumed to be the school and Internet. High school students, except for those who studied in the informatics department, have only two elective courses related to IT which are "information and communication technology" and "project preparation". The "Information and communication technology" course has two textbooks with the same title as the course and with almost identical content (Balaman, 2013; Eroğlu, & Yazar, 2013). In the textbooks, security is mentioned, but how to ensure the security of IT resources is not addressed. The security part of the books contains information about information theft, using updated antivirus, turning firewall on, back up, using password, viruses, virus types, information lost and copyright. However, they do not include information about how to setup and manage the security settings of IT resources. The literature and examined projects show that online support studies most frequently are about Internet security.

From the analysis of the findings about students' current resources in IT security, it can be concluded that high school students may lack knowledge and skills about technical

settings of IT security. Since students in the informatics department take advanced courses (MoNE, 2011) about IT tools, they were not included in the current study.

In this phase, content and topics to be covered from the security settings were selected. Expert opinion about the appropriateness of the selected topics and content validity was obtained. A table of specifications (ToS) was created to link the selected content to the items in the questionnaires. The final version of the ToS (see Appendix C) included topics of the study, related content links on the SP and related questions in the questionnaire.

### **3.7.2.2. Design and Development of the SP**

One of the unstated aims of the study was that high school students would understand and use the specified settings presented in the SP.

In order to access the content anywhere and anytime, SP was designed as an online support tool. SP was designed as a platform to include videos/articles to present content sequentially, to ask questions, and to share experiences.

So as to have all the members of the development team, that is, the designer, software developer, and content developer to have a similar understandings of the structure of SP and the interoperation between content, design and functionality, a blueprint of the SP was designed (see Figure 3.1). SP has separate pages with functionalities for users and administrators. While the user page presents the content, the administration page was designed to manage the content, comments, members, and reports sections of the SP.



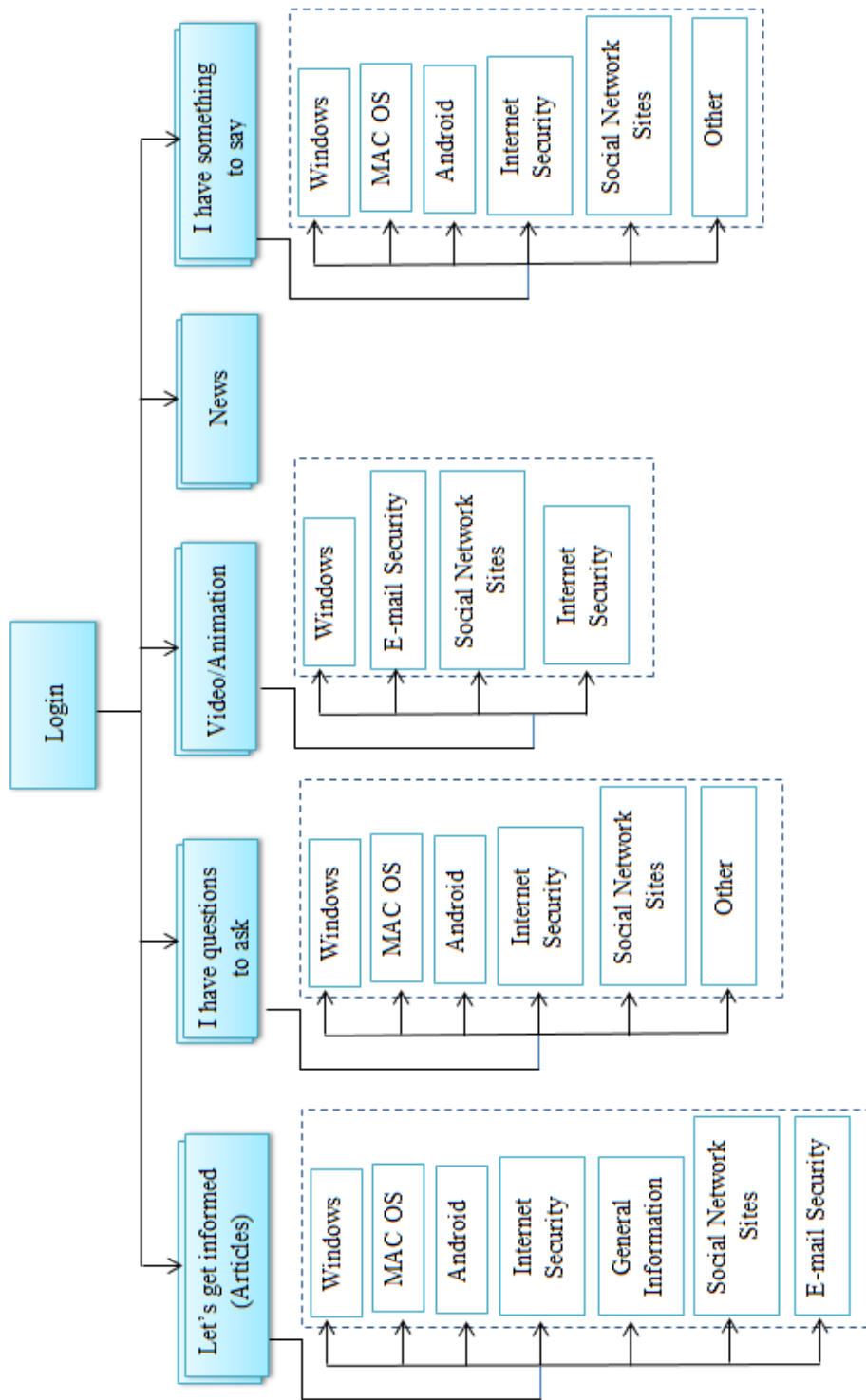


Figure 3.1 Blueprint of the SP.

The second level subtopics under “Let’s get informed” and “Video/Animation” are given in Table 3.4. The code of the first level subtopic content is as follows: Windows OS is 1; MAC OS is 2; Android is OS 3; Social Networking Sites is 4; E-mail Security is 5; Internet Security is 6; and General Information is 7.

Table 3.4 Second level subtopics under “Let’s get informed” and “Video/Animation”

|   | 1       | 2   | 3   | 4   | 5   | 6   | 7   |
|---|---------|-----|-----|-----|-----|-----|-----|
| Creating user account                     | (*)     |     |     |     |     |     |     |
| Adding password to user account           | (*),(+) | (*) | (*) |     |     |     |     |
| Defender                                  | (*)     |     |     |     |     |     |     |
| Safe Mode                                 | (*)     |     |     |     |     |     |     |
| Firewall                                  | (+)     |     |     |     |     |     | (*) |
| Adding password to screensaver            | (+)     |     |     |     |     |     |     |
| Updating the Windows Sandbox              | (+)     | (*) |     |     |     |     |     |
| FileVault                                 |         | (*) |     |     |     |     |     |
| Finding Missing MAC OS Password Assistant |         | (*) |     |     |     |     |     |
| Settings WiFi and Bluetooth of Android OS |         |     | (*) |     |     |     |     |
| Android OS screen lock                    |         |     | (*) |     |     |     |     |
| Facebook and Twitter                      |         |     |     | (*) |     |     |     |
| Changing Facebook password                |         |     |     | (*) |     |     |     |
| Changing Twitter password                 |         |     |     | (*) |     |     |     |
| Facebook & Twitter Privacy Settings       |         |     |     | (*) |     |     |     |
| How to use e-mail                         |         |     |     |     | (*) |     |     |
| G-mail password setting                   |         |     |     |     | (*) |     |     |
| Hotmail password setting                  |         |     |     |     | (*) |     |     |
| Netsmartz videos (8 videos)               |         |     |     |     |     | (*) |     |
| Browser security                          |         |     |     |     |     | (+) |     |
| Safe online shopping                      |         |     |     |     |     |     | (*) |
| IT security terms                         |         |     |     |     |     |     | (*) |
| What is IT crime?                         |         |     |     |     |     |     | (*) |

Table 3.4 (cont'd)

|  |     |
|--|-----|
| What is firewall?                                  | (*) |
| What is the user account?                          | (*) |
| What is the operating system?                      | (*) |
| Safe internet usage rules (parent-child agreement) | (*) |
| Secure internet usage policies                     | (*) |

---

(\*) indicates content is available under the “Let’s get informed” menu

(+) indicates content is available under the “Video/Animation” menu

SP was developed in Turkish because the target groups’ native language is Turkish. It was published on the World Wide Web with the domain name “Conscious Person (Bilinçli Birey)” to highlight the aim. The domain name had a semantic relation with the content it presented and it was easy to recall (<http://bilinclubirey.com/>). SP was designed so as to have separate interfaces for students, families, and teachers. Each separate interface had its own characteristic images related to the target user group. The login page of the SP was designed to give a message to the user about the importance of the authentication.

As shown in Figure 3.2, the user was welcomed with a banner pointing at the importance of authentication and password selection: “*Conscious Persons’ IT devices cannot be logged onto without a password.*”

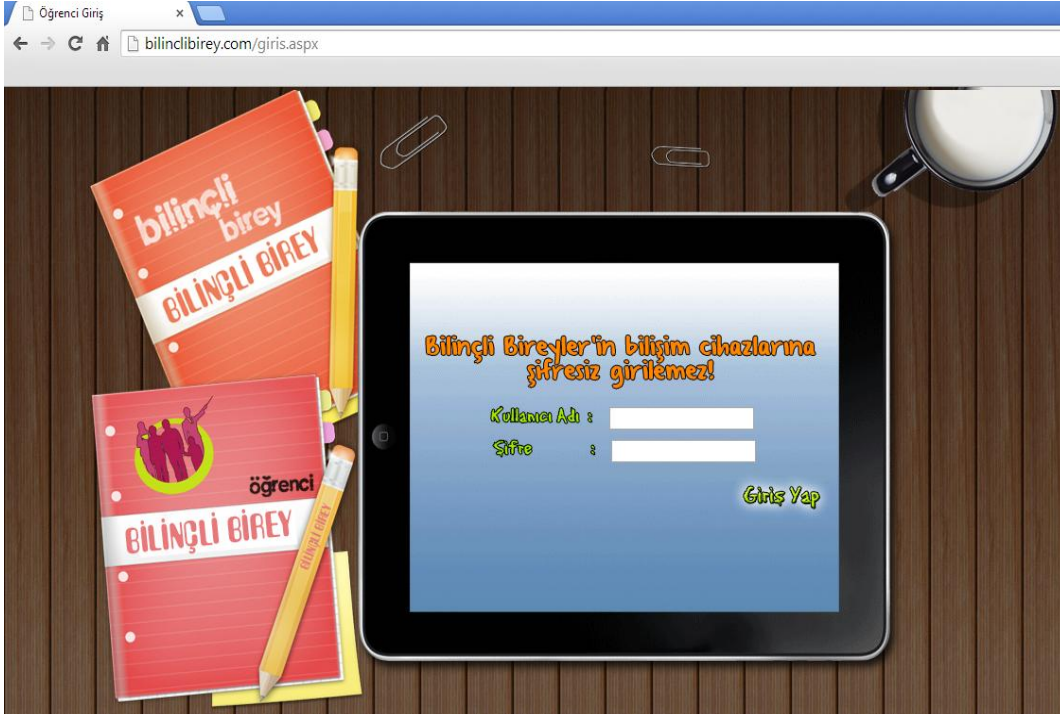


Figure 3.2 A screenshot from login page of SP.

High schools students and adults/parents from the designer's and researcher's work and living environment were asked to provide comments on the design. These comments were taken into account to finalize the design of the SP. The homepage of the SP is shown in Figure 3.3.



Figure 3.3 A screenshot from the homepage of the

Post-its' were used to remind users to perform basic actions for IT security. Notes on post-its were "Do not open every e-mail!", "Do not save or write down the password.", "Password is the main security step.", "Do not forget to update the system.", "Forbidding the internet is not a solution." Icons were used as menu to organize the different presentation of the content:

“Let’s Get Informed (Bilgilenelim)””: In case of using SP via mobile devices “Technological Constraints of Mobiles” was also taken into consideration to minimize the restrictions of mobile devices (Damaševičius, 2009). Damaševičius (2009) lists these constraints as limited input facilities, small screen size, low resolution and number of colors, slower CPU and smaller memory, lack of persistent storage, battery life, and data connectivity. In order to minimize restrictions of the mobile devices related to these constraints, content given as video/animation was also given as articles. “Let’s Get Informed” included articles about IT security and technical security settings of IT resources. The content was grouped according to the main topics, which were Windows, MAC OS X, Android, Internet Security, General Information, and Social Networking Sites. Design of the “Let’s Get Informed” is as shown in Figure 3.4.

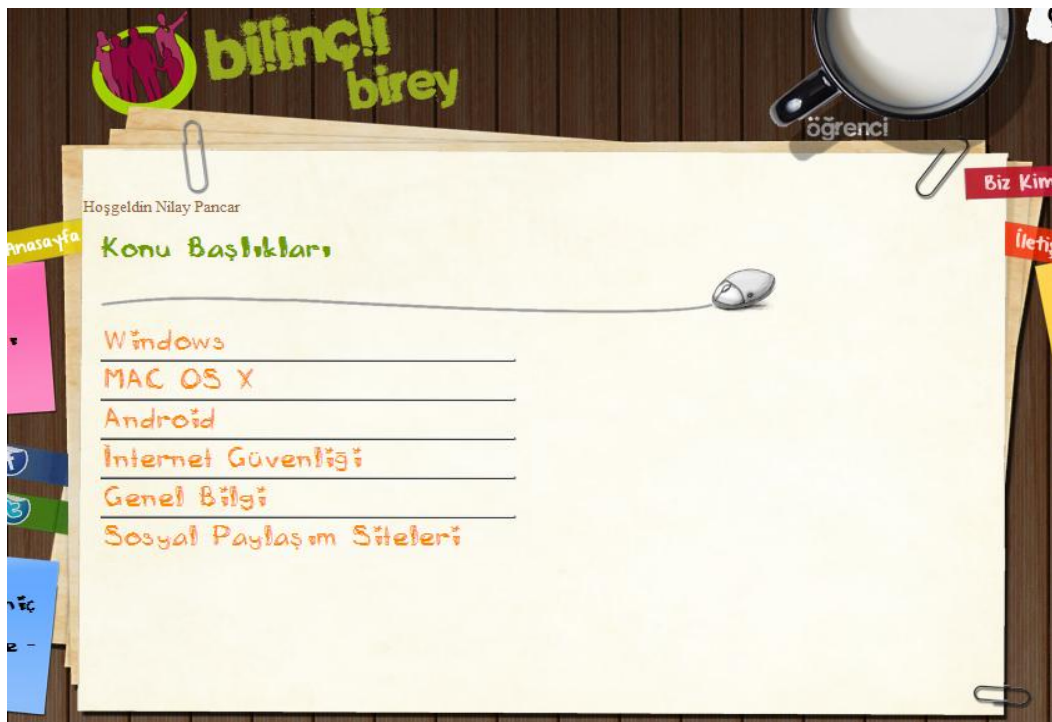


Figure 3.4 A screenshot from the *Let’s Get Informed* menu.

The “Full Screen” (Tam Ekran) option was added to the right top side of the articles to minimize the constraints of small screen size (Damaševičius, 2009). The design of the articles in “Let’s Get Informed” is as shown in Figure 3.5.



Figure 3.5 Screenshot from article about the privacy settings of SNSs.

“Video/Animation (Video/Animasyon)”: This part was designed to watch videos/animations about the importance of IT security and about how to manage the security settings of IT tools. Videos were also uploaded to Youtube in case of any problems which may occur due to OSs. A “full screen icon” was added to the videos to minimize the constraints of small screen size (Damaševičius, 2009). Design of the videos in “Video/Animation” is as shown in Figure 3.6.



Figure 3.6 Screenshot from video about the screensaver settings of Windows.



The “I have questions to ask (Soracaklarım var)” menu was designed to enable users to ask questions about IT security to experts. Questions could be answered by administrators as experts or by other users. Questions and answers are checked by the administrator before they are published on the SP. Inappropriate questions are not approved for publication. Design of the questions and answers in “I have questions to ask” is as shown in 3.7.

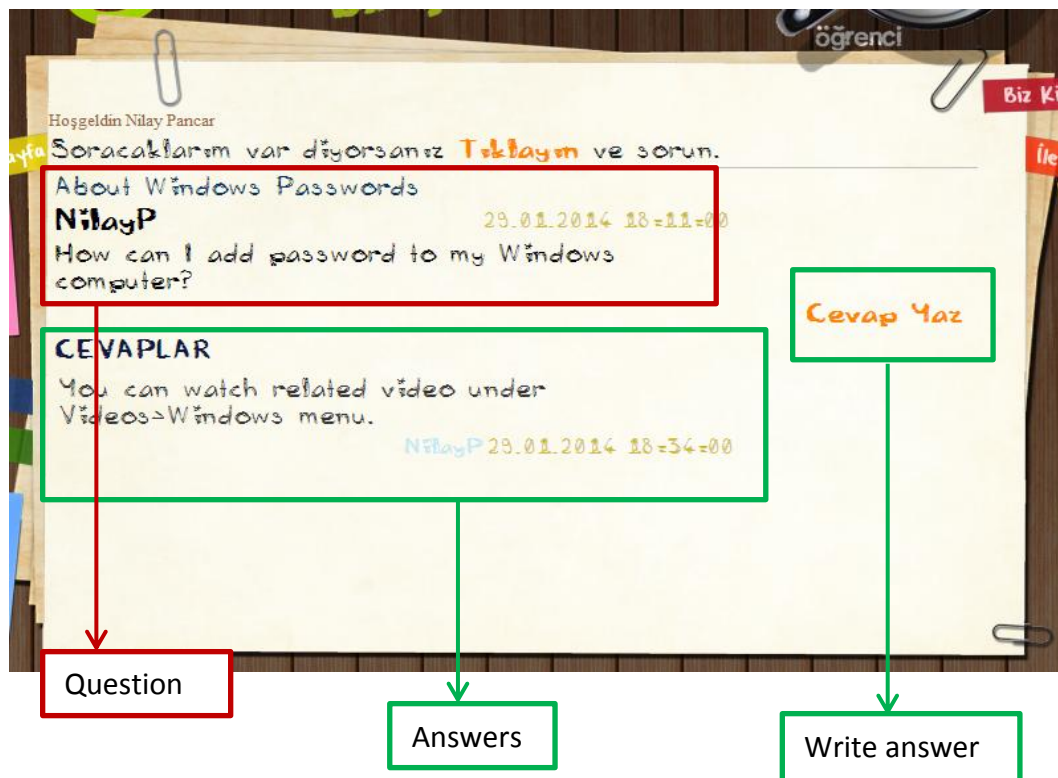


Figure 3.7 Screenshot from published question and answers with explanations.

“*News (Haberler)*”): This section was designed to inform students about new threats, risks, new protection methods, etc.

“*I have something to tell (Anlatacaklarım Var)*”): This section was designed to give students the opportunity to share their experiences.

The security portal has a separate administration section to manage the content, ask and answer questions, and to create reports about the users (see Figure 3.8).



Figure 3.8 A screenshot from the administration page

### 3.7.2.3. Coding of SP and Content Development

SP was designed as a dynamic server-side web site. Asp.net and SQL database were used to create SP. SP was hosted at the server located at Middle East Technical University campus. Authentication control was used to prevent entrance by unauthorized users. Users can only access the profile that they are authorized to. Since the logged time was important for the current study, automatic logoff was added to SP. Before introducing SP to the users, SP was tested for any problems.

Content was as important as the user interface design of SP. The content developer used the following questions before deciding on the content to be included.

- 1- Which security settings should students know to ensure IT security?
- 2- How can the content be presented more comprehensibly?
- 3- How can accurate information be provided?

The first question was about the content to be presented to the portal users. Expert opinions, online research, and technical specification documents (Apple Inc., 2010; Microsoft Safety & Security Center, 2004) were used to decide on the content. The main topics selected to be included in the portal were:

- Operating systems
  - Windows
  - MAC OS X
  - Android
- Social Networking Sites
- E-mails
- Web browsers
- IT terms

A table of specifications (ToS) was prepared to present subtopics in a meaningful structure and to ensure that all selected IT security settings were included and had a corresponding link on the SP. The second question was about how the content can be delivered to the students. One of the possible benefits of the current study was to support high school students to gain the required knowledge and skills in IT security. Participants' knowledge and skills in IT security were assumed to be of different level. The content of SP included tasks that needed processes which require knowledge and skills to be followed. In the light of these needs, procedural learning is most appropriate to present the content to all participants at different knowledge and skill levels. Procedural learning includes Reigeluth's Approach and Carroll's Minimalist Approach (Çağiltay, 2011). In the current study, task analysis, presentation, practice, and feedback components of Reigeluth's Approach were followed (Çağiltay, 2011).

#### *Task Analysis:*

Task analysis requires examining the steps of the procedure to make sure that they are correct and feasible. Breaking down some steps into smaller steps is important since the learner might be unfamiliar with the steps (Çağiltay, 2011). While preparing the security settings, this component was taken into consideration. For instance, instead of the "open control panel" direction, the "go to start menu and click control panel" direction was used.

#### *Presentation:*

The presentation component suggests presenting the task in different ways such as via text or pictures (pamphlet, textbook, poster, web site, illustrated strip), audio (instructions on how to use voice-mail), or video (demonstrations of techniques, shots of necessary equipment) (Çağiltay, 2011). Reducing the reading and allowing users to start immediately on a meaningful task is also recommended to support learner-directed activities and accomplishment (Ismail, Rahman, Hassan, & Mahmud, 2008). In the current study, videos with step by step narration and articles with screen shots were preferred to present the content.

*Practice:*

“Exercises for practice should be as close as possible to the real-world task” (Çağiltay, 2011). The videos were recorded from real tasks, and articles also included steps and pictures of real tasks. Participants of the current study were assumed to be able to apply the steps on their own.

*Feedback:*

The main aim of the feedback component is to help the learner to fix a problem that may occur in any step of the procedure (Çağiltay, 2011). On the SP, the part (“*I have questions to ask*”) was added to allow participants to ask questions about IT security and problems they might have while applying steps of security settings procedures.

The third question was about creating the content. Except for MAC OS, the content of the subtopics -Windows, Android, SNSs, e-mails, web browsers, and IT terms- were created by the researcher. The Security Configuration guide published by Apple Inc. (2010) was used to create the subtopics and content of the subtopics related to MAC OS.

Videos and animations related to online behaviors were adopted from Netsmartz with permission. The following videos were translated and used in the portal:

- *Post-to-be Private:* The video is about setting SNS profiles and blogs to private, being careful about friend list, sharing the photos or videos only with people on one’s friend list, and not to share information about plans or whereabouts.
- *Broken friendship:* The video is about a friendship that was broken when a teen gave her best friend's mail password to other girls at school and their malicious use of this e-mail. The bad consequences of sharing a password were illustrated with a real story.
- *Amy’s Choice:* The video was about a true story of a 15-year-old girl who left home to meet with a man she first "met" online and consequences of this trust.

- *Julie's Journey*: The video was about a girl's online relationship with a convicted murderer and consequences of this relationship.
- *Bad Netiquette Stings*: Netiquette was designed as a word used to describe the good manners that people use online. The aim was to teach the term Netiquette and to adopt good manners in the online environment.
- *Don't Open That File*: The animation was about viruses that spread via e-mail attachments or downloaded files, and antiviruses.
- *Know the Rules*: The animation was about online rules.
- *The Boy Who Loves IM*: The animation was about teaching children not to share personal information such as address, telephone number, parents' work address/telephone number, or the name and location of their school.
- *Miketosis*: The animation informed children about how fast information spread in the online environment and the impossibility of controlling this spread. The animation also aimed to create knowledge about not sharing other people's information as it might hurt them.

In order to make SP a brand and to sustain its continuity, every material on SP had a watermark of the logo and/or name of the project (Bilinçli Birey).

## **CHAPTER 4**

### **RESULTS**

#### **4.1. Demographic Information about the Participants**

The purpose of giving demographics is to provide information about participants of the study and create a base for the analysis. The demographic information of the students was categorized in five groups: IT devices used by students, OSs used by students, SNSs used by students, web browsers used by students, and e-mail services used by students. Demographic information about the participants is shown in Table 4.1. Participants were allowed to mark more than one choice. As shown in Table 4.1, all of the participants used at least one IT resource. Twenty seven (10.4%) of the participants did not use SNSs, and 10 (3.8 %) did not use e-mail.

Table 4.1 Initial characteristic of the students

| IT Devices Used by Students (Q5)   | <i>f</i> | %    | n   |
|------------------------------------|----------|------|-----|
| Own computer                       | 159      | 60.5 | 263 |
| Computer in common use with family | 141      | 53.6 | 263 |
| Computer in the school laboratory  | 41       | 15.6 | 263 |
| Tablet PC                          | 78       | 29.7 | 263 |
| Smart phone                        | 207      | 78.7 | 263 |
| Other                              | 5        | 1.9  | 263 |
| <b>Used OS</b>                     |          |      |     |
| Windows                            | 248      | 94.3 | 263 |
| MAC OS                             | 5        | 1.9  | 263 |
| iOS                                | 56       | 21.3 | 263 |
| Android                            | 164      | 62.4 | 263 |
| Linux                              | 13       | 4.9  | 263 |
| Other                              | 7        | 2.7  | 263 |
| <b>Used SNSs</b>                   |          |      |     |
| I don't use SNSs                   | 27       | 10.4 | 263 |
| Facebook                           | 208      | 80.0 | 263 |
| Twitter                            | 122      | 46.9 | 263 |
| Other                              | 56       | 21.5 | 263 |
| <b>Used web browser</b>            |          |      |     |
| Internet Explorer                  | 44       | 16.8 | 263 |
| Chrome                             | 234      | 89.3 | 263 |
| Firefox                            | 41       | 15.6 | 263 |
| Safari                             | 33       | 12.6 | 263 |
| Other                              | 19       | 7.3  | 263 |
| <b>Used e-mail service</b>         |          |      |     |
| I don't use e-mail                 | <i>f</i> | %    |     |
| I don't use e-mail                 | 10       | 3.8  | 263 |
| Hotmail                            | 205      | 78.2 | 263 |
| Gmail                              | 162      | 61.8 | 263 |
| Yahoo                              | 15       | 5.7  | 263 |
| Other                              | 10       | 3.8  | 263 |



## 4.2. IT Security Rules and Being Informed

As shown in Table 4.2, 164 (62.4%) of the total participants reported that there were no written rules related to computer and internet use at school; and 99 (37.6%) reported that there were written rules related to computer and internet use at school. Of the participants, 164 (62.4%) reported that there were no written rules related to computer and internet use at home.

Table 4.2 Rules at school and at home about usage of IT devices

| Written IT rules at school   | <i>f</i> | %    | n   |
|--|----------|------|-----|
| There are not written rules on computer and internet use at the school.                                    | 164      | 62.4 | 263 |
| The usage and intended use of the school computers is specified.   | 61       | 61.6 | 99  |
| The intended use of the school internet is specified.  | 52       | 52.5 | 99  |
| In the case of problem with the computer the contact person was specified.                                 | 22       | 22.2 | 99  |
| <hr/>  |          |      |     |
| IT rules at home   |          |      |     |
| There are no rules on computer and internet use.   | 164      | 62.4 | 263 |
| There are rules on daily use hours.  | 39       | 39.4 | 99  |
| There are rules on downloading or copying files from internet, CD, DVD or flash memory without permission. | 13       | 13.1 | 99  |
| There are rules on speaking with strangers.  | 33       | 33.3 | 99  |
| There are rules on sharing personal information such as name, surname, age, phone number, and address.     | 49       | 49.5 | 99  |
| There are rules on e-mails from strangers.   | 21       | 21.2 | 99  |
| There are rules on attitudes and behaviors at the online environment.                                      | 27       | 27.3 | 99  |

Table 4.2 (cont'd)

|  |    |      |    |
|--|----|------|----|
| There are rules on set up programs without permission. | 20 | 20.2 | 99 |
| There is information about using approved web sites.   | 19 | 4.9  | 99 |

A Likert type scale was used to obtain frequencies about being informed by school or parents about IT security, which are shown in Figure 4.1. The majority of the students reported that they were not informed by the school about IT security, while 70 (26.6%) of the students reported that they were not informed about IT security by their parents.

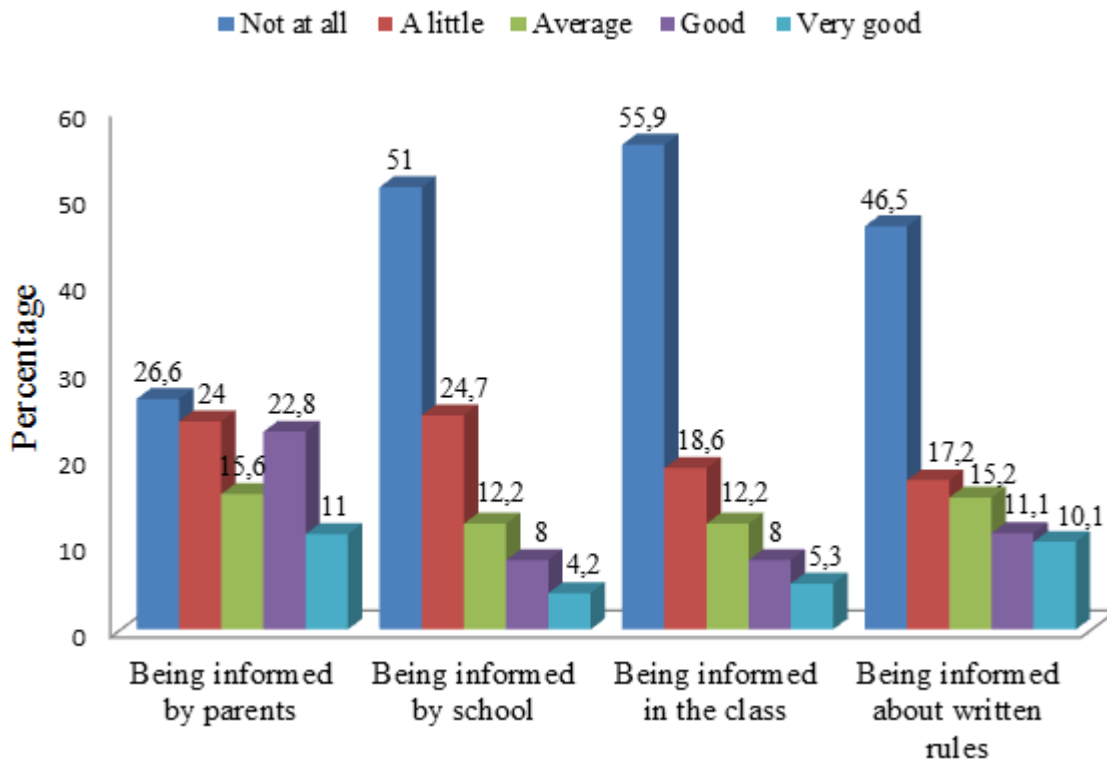


Figure 4.1 Response percentages to questions about being informed by school or parents about information security.

The questionnaire included questions about written rules at school. These questions were about being informed about written rules, accessibility, and comprehensibility of the written rules. Students who marked “There are no written rules about computer and internet use at school.” were excluded from the results related to written rules. More than 50% of the participants reported that they were not informed about written rules or only “a little” or at “average” level. The great majority of the students who reported that there were rules at school rated accessibility and comprehensibility of the written rules below “good” level. (see Figure 4.2).

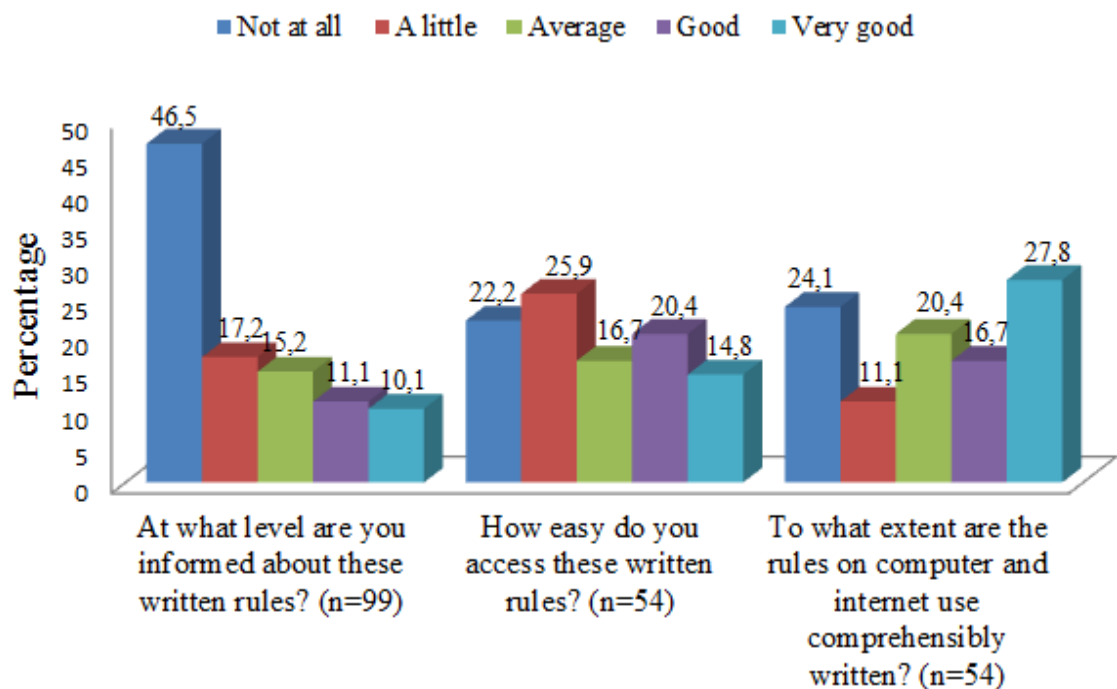


Figure 4.2 Response percentages to questions about written IT rules at school.

#### 4.3. Study Results on Research Questions 1 and 2

Most of the teachers reported their initial perceived knowledge and skills in IT security to be below “good” level, except for proper use of e-mail (see Table 4.3).

Table 4.3 Teachers' initial perceived knowledge and skills in IT security

| Question  | <i>f</i>  |               |           |           |            | n  |
|---|-----------|---------------|-----------|-----------|------------|----|
|   | 1         | 2             | 3         | 4         | 5          |    |
| <b>Knowledge level related to:</b>                    |           |               |           |           |            |    |
| IT crimes (Q13)                                       | 3 (13.6%) | 9 (40.9%)     | 4 (18.2%) | 3 (13.6%) | 13 (13.6%) | 22 |
| How to deal with IT crimes (Q14)                      | 4 (18.2%) | 10<br>(45.5%) | 4 (18.2%) | 3 (13.6%) | 1 (4.5%)   | 22 |
| Harms of unlicensed software (Q15)                    | 8 (36.4%) | 4 (18.2%)     | 5 (22.7%) | 4 (18.2%) | 0          | 21 |
| Criminal liability of using unlicensed software (Q16) | 9 (40.9%) | 4 (18.2%)     | 5 (22.7%) | 3 (13.6%) | 0          | 21 |
| <b>Perceived knowledge level related to:</b>          |           |               |           |           |            |    |
| Adding password to the screensaver of used OS (Q21)   | 4 (18.2%) | 4 (18.2%)     | 3 (13.6%) | 1 (4.5%)  | 0          | 12 |
| Creating user accounts (Q22)                          | 3 (13.6%) | 4 (18.2%)     | 1 (4.5%)  | 0         | 0          | 11 |
| Adding password to the OS (Q23)                       | 3 (13.6%) | 3 (13.6%)     | 5 (22.7%) | 1 (4.5%)  | 0          | 12 |
| Updating used OS (Q24)                                | 8 (36.4%) | 7 (31.8%)     | 3 (13.6%) | 2 (9.1%)  | 1 (4.5%)   | 21 |
| Windows firewall (Q25)                                | 7 (31.8%) | 7 (31.8%)     | 5 (22.7%) | 3 (13.6%) | 0          | 22 |
| Windows defender (Q26)                                | 9 (40.9%) | 5 (22.7%)     | 6 (27.3%) | 2 (9.1%)  | 0          | 22 |

Table 4.3 (cont'd)

|   |           |           |           |            |            |    |
|---|-----------|-----------|-----------|------------|------------|----|
| Settings menu of the Android OS (Q32)                   | 7 (70.0%) | 2 (20.0%) | 1 (10.0%) | 0          | 0          | 10 |
| Screen lock of the Android OS (Q33)                     | 7 (70.0%) | 2 (20.0%) | 1 (10.0%) | 0          | 0          | 10 |
| Adding owner information to the Android OS (Q34)        | 7 (70.0%) | 2 (20.0%) | 1 (10.0%) | 0          | 0          | 10 |
| Opening e-mails from strangers (Q35)                    | 3 (13.6%) | 1 (4.5%)  | 3 (13.6%) | 5 (22.7%)  | 1 (4.5%)   | 10 |
| Opening attachments in the e-mails from strangers (Q36) | 3 (13.6%) | 3 (13.6%) | 3 (13.6%) | 4 (18.2%)  | 0          | 13 |
| Opening attachments of the e-mails from strangers (Q37) | 13 (5.3%) | 14 (5.7%) | 24 (9.7%) | 54 (21.9%) | 142 (58%)  | 13 |
| Filtering settings of e-mails (Q38)                     | 0         | 1 (4.5%)  | 1 (4.5%)  | 4 (18.2%)  | 15 (68.2%) | 21 |
| Security settings of web browsers (Q39)                 | 0         | 1 (4.5%)  | 2 (9.1%)  | 6 (27.3%)  | 12 (54.5%) | 21 |
| Harms of sharing personal information via SNSs (Q40)    | 0         | 2 (9.1%)  | 0         | 5 (22.7%)  | 14 (63.6%) | 21 |
| Security and privacy settings of SNSs (Q41)             | 4 (12.8%) | 8 (36.7%) | 5 (22.7%) | 3 (13.6%)  | 0          | 20 |

PSKiITSQ-1 was administered to 263 participants to determine the initial knowledge and skill level of the students and teachers. Since participants were requested to skip the questions related to IT resources that they do not use, the total number of participants responding to the questions was different. Participants rated their level of knowledge and skills on a 5-point Likert scale; 1 = Not at all. 2 = A little. 3 = Average. 4 = Good. 5 = Very good.

As shown in Table 4.4., most of the students ranked their perceived present knowledge and skills below “good” level, except for the items (i) security settings of Android OS, (ii) e-mail security, (iii) harms of sharing personal information and (iv) security & privacy settings of SNSs.

Table 4.4 Students’ initial perceived knowledge and skills of in IT security.

| Question                         | <i>f</i>      |               |               |               |              | n   |
|----------------------------------|---------------|---------------|---------------|---------------|--------------|-----|
|                                  | 1             | 2             | 3             | 4             | 5            |     |
| <b>Knowledge level in:</b>       |               |               |               |               |              |     |
| IT crimes (Q14)                  | 28<br>(10.6%) | 81<br>(30.8%) | 79<br>(30.0%) | 57<br>(21.7%) | 18<br>(6.8%) | 263 |
| How to deal with IT crimes (Q15) | 56<br>(21.3%) | 67<br>(25.5%) | 77<br>(29.3%) | 47<br>(17.9%) | 16<br>(6.1%) | 263 |

Table 4.4 (cont'd)

|  |               |               |               |               |               |     |
|--|---------------|---------------|---------------|---------------|---------------|-----|
| Harms of unlicensed software (Q16)                                       | 65<br>(27.7%) | 64<br>(24.3%) | 56<br>(21.3%) | 51<br>(19.4%) | 27<br>(10.3%) | 263 |
| Criminal liability of using unlicensed software (Q17)                    | 76<br>(28.9%) | 71<br>(27.0%) | 57<br>(21.7%) | 36<br>(13.7%) | 23<br>(8.7%)  | 263 |
| <b>At what level:</b>  |               |               |               |               |               |     |
| Do your parents inform you about information security? (Q18)             | 70<br>(26.6%) | 63<br>(24.0%) | 41<br>(15.6%) | 60<br>(22.8%) | 29<br>(11.0%) | 263 |
| Does your school inform you about information security? (Q19)            | 134<br>(51%)  | 65<br>(27.7%) | 32<br>(12.2%) | 21<br>(8.0%)  | 11<br>(4.2%)  | 263 |
| Are you informed about computer use in the class? (Q20)                  | 147<br>(56%)  | 49<br>(18.6%) | 32<br>(12.2%) | 21<br>(8%)    | 14<br>(5.3%)  | 263 |
| Are you informed about these written rules? (Q21)                        | 37<br>(38.5%) | 19<br>(19.8%) | 17<br>(17.7%) | 14<br>(14.6%) | 9<br>(9.4%)   | 96  |
| How easy do you access these written rules? (Q22)                        | 36<br>(37.5%) | 14<br>(14.6%) | 16<br>(16.7%) | 14<br>(14.6%) | 16<br>(16.7%) | 96  |
| Are the rules on computer and internet use comprehensibly written? (Q23) | 33<br>(34.5%) | 18<br>(18.8%) | 15<br>(15.6%) | 14<br>(14.6%) | 16<br>(6.1%)  | 167 |

Table 4.4 (cont'd)

| <b>Perceived knowledge level on</b>                 |               |               |               |                             |                             |     |
|---|---------------|---------------|---------------|-----------------------------|-----------------------------|-----|
| Adding password to the screensaver of used OS (Q25) | 53<br>(20.5%) | 48<br>(18.5%) | 44<br>(16.7%) | 53<br>(20.5%)               | 60<br>(23.2%)               | 259 |
| Creating user accounts (Q26)                        | 21<br>(8.1%)  | 34<br>(13.1%) | 42<br>(16.2%) | 86<br>(33.2%)               | 75 (29%)                    | 259 |
| Adding password to the OS (Q27)                     | 46<br>(17.8%) | 41<br>(15.8%) | 51<br>(19.7%) | 58<br>(22.4%)               | 62<br>(23.9%)               | 259 |
| Updating used OS (Q28)                              | 34<br>(13.2%) | 45<br>(17.5%) | 47<br>(18.3%) | 65<br>(25.3%)               | 65<br>(25.3%)               | 257 |
| Windows firewall (Q29)                              | 56<br>(23.4%) | 44<br>(18.4%) | 41<br>(17.2%) | 61<br>(25.5%)               | 37<br>(15.5%)               | 239 |
| Windows defender (Q30)                              | 120<br>(50%)  | 27<br>(11.5%) | 34<br>(14.2%) | 35<br>(14.6%)               | 23<br>(9.6%)                | 239 |
| Settings menu of the Android OS (Q36)               | 5<br>(3%)     | 15<br>(9.1%)  | 28<br>(17.1%) | <b>55</b><br><b>(33.5%)</b> | <b>61</b><br><b>(37.2%)</b> | 164 |
| Screen lock of the Android OS (Q37)                 | 6<br>(3.7%)   | 14<br>(8.5%)  | 22<br>(13.4%) | <b>42</b><br><b>(25.6%)</b> | <b>80</b><br><b>(48.8%)</b> | 164 |



Table 4.4 (cont'd)

|   |               |               |               |                             |                             |     |
|---|---------------|---------------|---------------|-----------------------------|-----------------------------|-----|
| Adding owner information to the Android OS<br>(Q38)     | 10<br>(6.1%)  | 24<br>(14.6%) | 27<br>(16.5%) | <b>41</b><br><b>(25%)</b>   | <b>62</b><br><b>(37.8%)</b> | 164 |
| Opening e-mails from strangers (Q39)                    | 26<br>(10.5%) | 32<br>(13.0%) | 21<br>(8.5%)  | <b>66</b><br><b>(26.4%)</b> | <b>102</b><br><b>(41%)</b>  | 247 |
| Opening links in the e-mails from strangers<br>(Q40)    | 12<br>(4.9%)  | 11<br>(4.5%)  | 29<br>(11.7%) | <b>52</b><br><b>(21.1%)</b> | <b>143</b><br><b>(60%)</b>  | 247 |
| Opening attachments of e-mails from strangers<br>(Q41)  | 13<br>(5.3%)  | 14<br>(5.7%)  | 24<br>(9.7%)  | <b>54</b><br><b>(21.9%)</b> | <b>142</b><br><b>(58%)</b>  | 247 |
| Filtering settings of e-mails (Q42)                     | 65<br>(26.3%) | 46<br>(18.6%) | 43<br>(17.4%) | 62<br>(25.1%)               | 31<br>(12.6%)               | 247 |
| Security settings of web browsers (Q43)                 | 32<br>(12.7%) | 39<br>(15.5%) | 55<br>(21.9%) | 65<br>(25.9%)               | 60<br>(23.9%)               | 251 |
| Harms of sharing personal information via<br>SNSs (Q44) | 21<br>(8.4%)  | 36<br>(14.3%) | 47<br>(18.7%) | <b>79</b><br><b>(31.5%)</b> | <b>68</b><br><b>(27.1%)</b> | 251 |
| Security and privacy settings of SNSs (Q45)             | 23<br>(9.2%)  | 42<br>(16.7%) | 51<br>(20.3%) | <b>71</b><br><b>(28.3%)</b> | <b>64</b><br><b>(25.5%)</b> | 251 |

#### 4.4. Study Results on Research Question 3

The Wilcoxon signed-rank test was conducted to determine if the changes in students' perceived knowledge and skills in IT security was statistically significant. The measurement scale in the survey was a 5-point Likert scale; 1 = Strongly disagree. 2 = Disagree. 3 = Partly agree. 4 = Agree. 5 = Strongly agree.

Since participating in the current study was voluntary, PKSoITS-2 was applied to 132 students who attended to PKSoITS-1 and used SP. The Wilcoxon signed-rank test was performed to understand whether there was a statistically significant change between participants' PSKiITSQ-1- and PSKiITSQ-2 results after using the SP. Tables related to the analysis can be found in Appendix F.

The current study results for knowledge level of perceived knowledge of students in virus infections are as shown in Table 4.5. The current study results indicate that there was a positive change in participants' perceived knowledge in virus infections before and after SP use and this change was statistically significant.

Table 4.5 Students' perceived knowledge in virus infections results before and after SP use.

|   | <i>Before</i> |          |           | <i>After</i> |          |           |
|---|---------------|----------|-----------|--------------|----------|-----------|
|   | <i>n</i>      | <i>M</i> | <i>SD</i> | <i>n</i>     | <i>M</i> | <i>SD</i> |
| Perceived knowledge level of the participants on virus infections (Q10) * | 132           | 0.83     | 0.381     | 132          | 0.96     | 0.192     |

\* mean difference was statistically significant at  $p < 0.05$ .

Questions about awareness level of the IT crimes and unlicensed products and knowledge and skills on security settings were grouped in to 6:

*Group 1: Perceived knowledge and skill level related to awareness level of the IT crimes and unlicensed products:*

The current study results for awareness level of the IT crimes and unlicensed products were as shown in Table 4.6. The results indicate that there was a positive change in participants' perceived awareness about IT crimes and unlicensed products before and after SP use and that this change was statistically significant. The most positive change was in perceived knowledge on criminal liability of using unlicensed software (Q17).

Table 4.6 Students' perceived awareness about IT crimes and unlicensed products results before and after SP use.

| Perceived awareness about IT crimes and unlicensed products                          | <i>Before</i> |          |           | <i>After</i> |          |           |
|--|---------------|----------|-----------|--------------|----------|-----------|
|  | <i>n</i>      | <i>M</i> | <i>SD</i> | <i>n</i>     | <i>M</i> | <i>SD</i> |
| Perceived knowledge level in IT crimes (Q14) *                                       | 132           | 3.01     | 1.088     | 132          | 3.65     | 0.933     |
| Perceived knowledge level on how to deal with IT crimes (Q15) *                      | 132           | 2.62     | 1.163     | 132          | 3.53     | 0.976     |
| Perceived knowledge level on harms of unlicensed software (Q16) *                    | 132           | 2.77     | 1.357     | 132          | 3.57     | 1.064     |
| Perceived knowledge level on criminal liability of using unlicensed software (Q17) * | 132           | 2.5      | 1.263     | 132          | 3.40     | 0.972     |

\* mean difference was statistically significant at  $p < 0.05$ .

*Group 2: Perceived knowledge and skill level related to the common security settings of the OSs:*

The current study results for perceived knowledge and skill level related to common security settings of the OSs were as shown in the Table 4.7. The results indicated that there was positive change in students' perceived knowledge and skill level related to common security settings of the OSs and this change was statistically significant.

Table 4.7 Students' perceived knowledge and skill level related to common security settings of OSs results before and after SP use.

| Perceived knowledge and skill level related to the security settings of OSs        | <i>Before</i> |          |           | <i>After</i> |          |           |
|--|---------------|----------|-----------|--------------|----------|-----------|
|  | <i>n</i>      | <i>M</i> | <i>SD</i> | <i>n</i>     | <i>M</i> | <i>SD</i> |
| Perceived knowledge level on adding password to the screensaver of used OS (Q25) * | 130           | 3.08     | 1.407     | 129          | 4.18     | 0.775     |
| Perceived knowledge level on creating user accounts (Q26) *                        | 130           | 3.58     | 1.244     | 130          | 3.90     | 0.897     |
| Perceived knowledge level on creating user accounts (Q27) *                        | 130           | 3.21     | 1.396     | 130          | 3.92     | 0.907     |
| Perceived knowledge level on creating user accounts (Q28) *                        | 130           | 3.30     | 1.401     | 130          | 3.71     | 0.927     |

\* mean difference was statistically significant at  $p < 0.05$ .

*Group 3: Perceived knowledge and skill level on security settings of Windows OS*

Current study results for perceived knowledge and skill level on security settings of Windows OS were as shown in the Table 4.8. The results indicated that there was positive change in students' perceived knowledge and skill level on security settings of Windows OS and this change was statistically significant.

Table 4.8 Students' perceived knowledge and skill level related to security settings of Windows OS results before and after SP use.

| Perceived knowledge and skill level related to the security settings of Windows | <i>Before</i> |          |           | <i>After</i> |          |           |
|---|---------------|----------|-----------|--------------|----------|-----------|
|   | <i>n</i>      | <i>M</i> | <i>SD</i> | <i>n</i>     | <i>M</i> | <i>SD</i> |
| Perceived knowledge level on Windows firewall (Q29) *                           | 120           | 2.88     | 1.447     | 120          | 4.04     | 0.854     |
| Perceived knowledge level on Windows defender (Q30) *                           | 120           | 2.15     | 1.370     | 120          | 3.47     | 1.092     |

\*mean difference was statistically significant at  $p < 0.05$ .

*Group 4: Perceived knowledge and skill level related to security settings of Android OS:*

The current study results for perceived knowledge and skill level related to security settings of Android OS are as shown in Table 4.9. The results indicate that, except for the item “adding owner information to the Android OS”, there was positive change in students’ perceived knowledge and skill level related to security settings of Android OS and this change was statistically significant. There was a positive change in 37 students’ knowledge related to adding owner information (Q38) but this change was not statistically significant ( $Z = -.194, p = .868 > .05$ ) (see Appendix F)

Table 4.9 Students’ perceived knowledge and skill level related to security settings of Android OS results before and after SP use.

| Perceived knowledge and skill level on security settings of Android | <i>Before</i> |          |           | <i>After</i> |          |           |
|---|---------------|----------|-----------|--------------|----------|-----------|
|   | <i>n</i>      | <i>M</i> | <i>SD</i> | <i>n</i>     | <i>M</i> | <i>SD</i> |
| Knowledge level on settings menu of the Android OS (Q36) *          | 85            | 3.86     | 1.135     | 85           | 4.67     | 0.565     |
| Knowledge level on screen lock of the Android OS (Q37) *            | 85            | 3.99     | 1.170     | 85           | 4.40     | 0.759     |
| Knowledge level on adding owner information to the Android OS (Q38) | 85            | 3.73     | 1.238     | 85           | 3.69     | 1.205     |

\* mean difference was statistically significant at  $p < 0.05$ .

*Group 5: Perceived knowledge and skill level related to the security settings of e-mail services:*

The current study results for perceived knowledge and skill level related to the security settings of e-mail services are as shown in Table 4.10. The results indicate that, except for “opening attachments of the e-mails from unknown senders”, there was a positive change in students’ perceived knowledge and skill level related to the security settings of e-mail services, and this change was statistically significant. There was a positive change in 39 students’ perceived knowledge related to opening attachments of e-mails from unknown senders (Q41) and this change was not statistically significant ( $Z = -.846$ ,  $p = .398 > .05$ ) (see Appendix F)

Table 4.10 Students’ perceived knowledge and skill level related to security settings of e-mail services results before and after SP use.

| Perceived knowledge and skill level on security settings of e-mail services      | <i>Before</i> |          |           | <i>After</i> |          |           |
|--|---------------|----------|-----------|--------------|----------|-----------|
|  | <i>n</i>      | <i>M</i> | <i>SD</i> | <i>n</i>     | <i>M</i> | <i>SD</i> |
| Knowledge level on opening e-mails from strangers (Q39) *                        | 123           | 3.66     | 1.41      | 123          | 4.72     | 0.551     |
| Knowledge level on opening attachments in the e-mails from strangers (Q40) *     | 123           | 4.18     | 1.09      | 123          | 4.67     | 0.649     |
| Knowledge level on opening attachments of the e-mails from unknown senders (Q41) | 123           | 4.19     | 1.121     | 123          | 4.29     | 1.099     |
| Knowledge level on filtering settings of e-mails (Q42)                           | 123           | 2.65     | 1.385     | 123          | 3.63     | 0.977     |

\* mean difference was statistically significant at  $p < 0.05$ .

*Group 6: Perceived knowledge and skill level related to security settings of web browsers and SNSs:*

Current study results for perceived knowledge and skill level related to the security settings of web browsers and SNSs are as shown in Table 4.11. The results indicate that, except for the security and privacy settings of SNSs, there was a positive change in students' perceived knowledge and skill level related to the security settings of browsers and SNSs, and this change was statistically significant. There was a positive change in 67 students' knowledge and skill level related to the security and privacy settings of SNSs (Q45), and this change was not statistically significant ( $Z = -5.411, p = .398 > .05$ ) (see Appendix F).

Table 4.11 Students' perceived knowledge and skill level related to security settings of web browsers and SNSs results before and after SP use.

| Perceived knowledge and skill level on security settings of web browser and SNSs    | <i>Before</i> |          |           | <i>After</i> |          |           |
|---|---------------|----------|-----------|--------------|----------|-----------|
|   | <i>n</i>      | <i>M</i> | <i>SD</i> | <i>n</i>     | <i>M</i> | <i>SD</i> |
| Perceived knowledge level on security settings of web browsers (Q43) *              | 125           | 3.34     | 1.351     | 123          | 4.72     | 0.551     |
| Perceived knowledge level on harms of sharing personal information via SNSs (Q44) * | 123           | 4.19     | 1.121     | 123          | 4.29     | 1.099     |
| Perceived knowledge and skill level on security and privacy settings of SNSs (Q45)  | 123           | 2.65     | 1.385     | 123          | 3.63     | 0.977     |

\* mean difference was statistically significant at  $p < 0.05$ .



The time students spent on the SP was not used to measure the effect of the SP on students' knowledge and skill level since students shared their user name and password with each other. The time spent on SP ranged between 5 and 60 minutes.

#### 4.5. Study Results on Research Question 4

The majority of the time devoted to the study was spent on design and development of the user interface and content of the SP. These efforts were rewarded. As shown in Table 4.12, more than 60% of the students rated SP satisfaction at “good” and “very good” level.

Table 4.12 Students' satisfaction level with SP.

| Question   | <i>f</i>    |              |               |               |               |
|--|-------------|--------------|---------------|---------------|---------------|
|  | 1           | 2            | 3             | 4             | 5             |
| The aim of the videos and articles in the SP is explained clearly (Q31). | 0<br>(0%)   | 10<br>(7.6%) | 21<br>(15.9%) | 60<br>(45.5%) | 41<br>(31.3%) |
| Information in the SP is instructive (Q32).                              | 1<br>(0.8%) | 3<br>(2.3%)  | 34<br>(25.8%) | 53<br>(40.2%) | 41<br>(21.1%) |
| Information in the SP is up-to-date (Q33).                               | 0<br>(0%)   | 12<br>(9.1%) | 18<br>(13.6%) | 59<br>(44.7%) | 42<br>(31.8%) |
| Information in the SP is sufficient to learn the content (Q34)           | 1<br>(0.8%) | 10<br>(7.6%) | 26<br>(19.7%) | 51<br>(38.6%) | 44<br>(33.3%) |
| Content in the SP is understandable (Q35)                                | 0<br>(0%)   | 9<br>(6.8%)  | 27<br>(20.5%) | 53<br>(40.2%) | 43<br>(32.6%) |
| Content in the SP is fluent (Q36)  | 1<br>(0.8%) | 6<br>(4.5%)  | 22<br>(16.7%) | 57<br>(43.2%) | 46<br>(34.8%) |

Table 4.12

|  |             |              |               |               |               |
|--|-------------|--------------|---------------|---------------|---------------|
| Security settings of the IT devices can be easily done by using information on the SP (Q37). | 1<br>(0.8%) | 5<br>(3.8%)  | 30<br>(22.7%) | 51<br>(38.6%) | 45<br>(34.1%) |
| Content in the SP is given by using appropriate methods (video. article) (Q38).              | 0<br>(0.8%) | 5<br>(3.8%)  | 29<br>(22.0%) | 62<br>(47.0%) | 36<br>(27.3%) |
| SP is designed in a way to access any content easily. (Q39)                                  | 0<br>(0.0%) | 5<br>(3.8%)  | 25<br>(18.9%) | 47<br>(35.6%) | 55<br>(41.7%) |
| Colours of the SP are well selected and do not strain eyes (Q40).                            | 1<br>(0.8%) | 6<br>(4.5%)  | 28<br>(21.2%) | 52<br>(39.4%) | 45<br>(34.1%) |
| Using SP is easy (Q40-56).   | 0<br>(0%)   | 9<br>(6.8%)  | 22<br>(16.7%) | 46<br>(34.8%) | 55<br>(41.7%) |
| SP is visually well designed (Q41).  | 1<br>(0.8%) | 9<br>(6.8%)  | 23<br>(17.4%) | 44<br>(33.3%) | 55<br>(41.7%) |
| Videos and articles in the SP load fast enough (Q42).  | 1<br>(0.8%) | 10<br>(7.6%) | 32<br>(24.2%) | 43<br>(32.6%) | 46<br>(34.8%) |
| Links in SP work smoothly (Q43)  | 1<br>(0.8%) | 5<br>(3.8%)  | 28<br>(21.4%) | 47<br>(35.9%) | 50<br>(38.2%) |

## CHAPTER 5

### DISCUSSION AND RECOMMENDATIONS

The aim of this chapter was to evaluate the findings. The major points of the result chapter were given to discuss and make recommendations. Finally, further implications were listed for future studies by considering the findings of the study.

#### 5.1. IT Rules at School and at Home

The results of the current study indicate that all student participants are using at least one IT device and more than 60% of the student participants are using their own devices. A great majority of the participants are using SNSs, web browsers and e-mail services. Similarly, Livingstone, Haddon, Görzig and Ólafsson (2011) reported that 75% of the students use social networking, instant messaging, and e-mail. Kaspersky (2013) and Symantec Corporation (2013) reports address that web-based and targeted attacks are increasing sharply. National Cyber Security Alliance (2014) revealed that great majority of the teen internet users have asked for or sought out advice on managing their privacy. These studies, in addition to the findings of the current study, indicate that increasing students' awareness and knowledge on privacy is becoming an important IT security issue.

Exposing students to Information Security issues is important to motivate their information security behaviors (Bagchi-Senet al., 2006). Therefore, students should be informed about the computer and internet rules. Explaining the rules is an important

point to ensure the IT security when students use them outside of the school (ETPRO-NCSA, 2008). However, in the current study a great majority of the participants (62.4%) reported that there are no rules on computer and internet usage at school. Participants who reported that there are rules about computer and internet at school mentioned that the rules are about usage and intended use of the school computers and the Internet. More than 60% of the students reported that being informed about written IT security rules, accessibility and comprehensibility of these rules are below “good” level. More than 80% of the students also reported that they are informed below “good” level about information security and computer use at school. Researchers claim that schools have fundamental role in ensuring students’ safety in online environment (Wishard, 2004; Valcke, Schellens, Van Keer, & Gerarts. 2007; Livingstone, Haddon, Görzig & Ólafsson, 2011). Therefore, schools in Turkey are responsible to inform students about MoNE’s circulars and guidelines which are called “Internet Ethic” and “Advices for Secure Usage of the Internet”. However, results of the current study are in line with the findings of ETPRO-NCSA (2008) that schools do not focus enough on the security issues since published IT security standards or circulars are not a part of curricula and they are not assessed. Additionally, students (56%) reported that they are not informed about computer use in class and results of the current study indicate that teachers do not have sufficient knowledge and skills about IT security. Findings of the current study and ETPRO-NCSA (2008, 2010) show that the extent of informing students in class may positively correlate with teachers’ knowledge and skills.

The results of the current study show that there are rules on computer and internet use in 37.6% of the participants’ home. Fifty (12.9%) of the participants reported that there are rules about e-mails from unknown senders. and 39 (10.1%) of the participants reported that there are rules about daily computer usage hours at home. According to Livingstone & Bober’s (2006) study, 42% of the children stated that they have rules for how long they can go online. The results of the current study and Livingstone and Bober’s (2006) study show that families’ common rule on computers is the computer and internet usage hours. The current study did not include families, and the findings of the current study

are only based on students' answers. Livingstone and Bober's (2006) study revealed an interesting situation: While 86% of the parents claim that they do not allow their child to give out their personal information, only 49% of the children say they are not allowed to give out their personal information. There are differences between parents and students' conception about the rules. For this reason, including families in the study is important.

## **5.2. Students' and Teachers' Initial Perceived Knowledge and Skill Level in IT Security (Refers to Research Question 1 and 2).**

Each end user needs to ensure his/her privacy and security. With this aim security awareness programs should be initiated to raise students' knowledge and skill level in IT security (Mensch & Wilkie, 2011). The results of the current study indicate that a great majority of the students are below "good" level at creating password for user account and screensaver of OSs. Ninety eight percent of the students reported that they use Windows OS; and more than half of these students rated their knowledge and skill on security settings of Windows below "good" level. Students also rated their knowledge and skills on security setting of e-mail and web browsers below "good" level. Another study conducted by Tekerek (2012) with 2447 students at Turkish schools similarly concluded that students' awareness about issues required knowledge such as using a strong password, scanning for malicious software, firewall, and filtering is at low level. The results of the current study and Tekerek's (2012) study results give insights to the Turkish Education System where classes related to IT are elective and do not include security settings of IT devices in a detailed way. To support students to improve their knowledge and skill on password management, comprehensible guidelines should be prepared and adopted; regular training sessions should be conducted at school and at home for routine use of these guidelines and for teaching how to configure security settings of IT tools (Mensch & Wilkie, 2011; Victory. 2003).

The National Center for Education Statistics (NCES) (n.d.) and Symantec Corporation's report (2013) indicate that privacy is an important issue of security and "Phishing" and

“Targeted Attacks” are top threats to data protection. “Phishing” and “Targeted Attacks” may occur due to inappropriate use of e-mail and sharing personal information unconsciously. Half of the students who participated in the current study reported that their knowledge and skills about e-mail security and the risks associated with use of e-mail attachments, and harms of sharing personal information are at “good” and “very good” level. Students’ knowledge and skills about appropriate use of e-mail might be affected by IT rules at home related to e-mails. The findings of the current study are consistent with Livingstone, Haddon, Görzig and Ólafsson’s (2011) study in which half of the students reported that they know privacy settings of e-mail and do not share personal information.

Since school is the second most common location at which students use the internet, teachers have an important role in supporting students to improve their knowledge and skills on safe and responsible use of the Internet (Livingstone et al. 2011). Livingstone et al. (2011) reported that 58% of the students receive advice from their teachers. According to the results of a study conducted with 1569 educators in 2008, the majority of the teachers do not have sufficient knowledge and skills about IT security and they do not feel comfortable to discuss safety issues with students (ETPRO-NCSA, 2008). The results of the current study also revealed that teachers’ perceived knowledge and skills in IT security issues are below “good” level. As concluded by ETPRO-NCSA (2008, 2010), if confidence of the educators increase in IT security, they feel more prepared to discuss IT security issues with the students.

### **5.3. Effect of SP on Students’ IT Security Knowledge and Skill Level (Refers to Research Question 3)**

Successful integration of the computers into education has important effects on students’ academic and future work life (OECD, 2005; Mueller. 2010). IT tools have numerous positive effects on education such as ease of access to information, improved simulation capabilities, enhanced productivity, and means to provide technology-based assistive

support (Barron, Kemker, KHarmes, & Kalaydjian, 2003; Chou & Peng, 2010; Peng & Ramaiah, 2007; ETPRO-NCSA, 2008). Furthermore, being familiar with different media common to the modern workplace will have positive effects at work (OECD, 2005). In addition to the benefits, unconscious or inappropriate usage of IT tools may result in vulnerabilities, risks, threats or attacks. The results of the current study indicate that except (i) adding owner information to IT devices with Android OS, (ii) risk associated with opening e-mails from unknown senders, (iii) and security-privacy settings of SNSs. SP has significant positive change in students' perceived knowledge and skills in IT security issues. The results of the current study are in support of Bagchi-Senet al.'s (2006) study which revealed that exposing students to the information about IT security increased their perceived knowledge and skill level in IT security. Chou and Peng (2011) in their study indicate that most frequent of the teachers (67.41%) used eteacher materials in their teaching practices and (67.41%) they stated that materials on eteacher positively changed students' knowledge, attitudes, or behaviors regarding their Internet usage. Supporting students to improve their knowledge and skills in IT security will help them protect themselves and ensure more safe and secure national infrastructure (ETPRO-NCSA, 2008). Regarding the findings of the current study, first of all a *Computer Technology Acceptable Use and Internet Policy* might be prepared for the nation and all schools might be forced to introduce it to the teachers, students and parents as in other countries (Victory, 2003; Wilson & Hash, 2003; McDaniel & Early, 2013). Elective courses related to IT might be must courses, and they might begin in kindergarten instead of one year guiding and might continue through 12<sup>th</sup> grade as in Pittsylvania County Schools (McDaniel & Early, 2013). Moreover, course content of IT classes needs to be revised and security issues need to be covered in a more detailed manner. Since technology develops rapidly with the aim of reducing the cost to publish textbooks and providing students with up-to-date information, online materials can be developed instead of textbooks with the aim of supporting the students, teachers and parents about IT security.

#### **5.4. Conclusion**

In the current study it is aimed to provide insight for further studies to examine present perceived knowledge and skills of the students' in IT security and how an online support tool affect high school students' knowledge and skill level in IT security. Based on the findings of the current study, it can be claimed that Turkish high school students' initial perceived awareness, knowledge and skills in IT security is not enough to protect themselves. The findings of the current study also show that online support tool may support students to improve their knowledge and skills in IT security.

Based on the findings of the current study, there are two recommendations that could form the basis for further research on supporting the students about IT security

- Make sure that many studies have not been carried out in the school you are going to work with to increase the response rate.
- While explaining the aim of the study to the students. do not forget emphasize that the amount of the time they spent on the online support tool is important for the study findings and warn them not to share their usernames and passwords with each other.

#### **5.5. Limitation of the Study**

Since the study was based on voluntary participation, convincing the schools, teachers, and students to participate in the study needed an extra effort. Teachers were reluctant to allocate time for the study since they needed the time to cover their course topics and students were reluctant to spend their break time on the study. Ensuring students to use the SP was another limitation since it was also voluntary. The results of the study were also limited with the honesty of students.



## **5.6. Implications for Research**

This study contributes to the literature by providing insight into the initial perceived knowledge and skills of Turkish students and teachers related to IT security, and the effect of an online support tool on students' perceived knowledge and skills in IT security. According to the results of the current study, some actions need to be taken to improve students' and teachers' knowledge and skills in IT security. In line with this aim, online support tools such as SP might have a significant effect on their knowledge and skills in IT security. The current study might be helpful for researchers, policy makers and educators in designing, developing, and implementing such online support tools. The current study also provides evidence about the inadequacy of IT courses with respect to ensuring IT security. SP might be used in the IT classes as a learning material.

Furthermore, many studies and projects try to determine the extent and adequacy of students', teachers' or parents' understanding of risky, unsafe, or unethical internet behaviors; and results of proactive actions were taken into consideration to increase students', teachers' or parents' awareness and knowledge in proper use of the Internet. Too little research has focused on awareness, knowledge, and skills in relation to the security settings of IT tools. The current study might be a valuable resource for researchers who wish to study ways of increasing citizens' knowledge and skills in IT security.

## **5.7. Suggestion for Further Research**

This study was conducted to figure out students' *perceived* knowledge and skills in IT security. Future research should determine if online support tool has an effect on students' knowledge and skill level in practice. For this aim students can be given tasks about the security settings of IT tools; and students' movement on the online support tool can be traced to examine the relationship between change in knowledge/skills and

online support tool. Furthermore, family support has a significant impact on students' computer self-efficacy and computer use (Hsiao, Tu, & Chung, 2012). Teachers and parents should be included to determine if their knowledge and skill level have an effect on students' knowledge and skill level in IT security. In Turkey, except high schools' informatics department, course content of IT classes at high school may not be enough to increase the students' knowledge and skills in IT security (Balaman, 2013; Eroğlu & Yazar, 2013). Further research may use the online support tool in the IT classes to give insights into the IT classes.

## REFERENCES

- An, Y., & Reigeluth, C. (2011). Creating technology-enhanced, learner-centered classrooms: K-12 teachers' beliefs, perceptions, barriers, and support needs. *Journal of Digital Learning in Teacher Education*, 28(2), 54-62
- Apple Inc. (2010). Mac OS X security configuration for MAC OS X version 10.6 snow leopard. Retrieved on June 15, 2012 from <https://ssl.apple.com/support/security/guides/>
- Atkinson, J., & Finn, T. (2009). Promoting the safe and strategic use of technology for victims of intimate partner violence: evaluation of the technology safety project. *Journal of Family Violence*, 24, 53-59. Retrieved on June 15, 2013 from <http://ww2.lib.metu.edu.tr/en/index.php>
- Bagchi-Sen, S., Chai, S., Morrell, C., Rao, H. R., & Upadhyaya, S. (2006). Role of perceived importance of information security: an exploratory study of middle school children's information security behavior. *Issues in Informing Science and Information Technology*, 3, 127-135.
- Bilgi Teknolojileri ve İletişim Kurulu. (2011). Güvenli İnternet Hizmetine İlişkin Usul Ve Esaslar Taslağı. 2011/DK-14/410. Retrieved on August 10, 2014 from [http://www.btk.gov.tr/mevzuat/kurul\\_kararlari/dosyalar/2011%20DK-14%20410.pdf](http://www.btk.gov.tr/mevzuat/kurul_kararlari/dosyalar/2011%20DK-14%20410.pdf)
- Balaman, Y. (2013). Ortaöğretim bilgi ve iletişim teknolojisi ders kitabı. Bahadır, H. (ed. Ankara: Fırat Yayıncılık. Retrieved on June 22, 2013 from <http://www.meb.gov.tr/duyurular/duyuruayrinti.asp?ID=10488>
- Barron, A. E., Kemker, K., Harmes, C., & Kalaydjian, K. (2003). Large-scale research study on technology in K-12 schools: Technology integration as it relates to the National Technology Standards. *Journal of Research on Technology in Education*, 35, 489-507. Retrieved on June 5, 2012 from <http://teachingtools2dot0.wikispaces.com/file/view/article%203.pdf/257508540/article%203.pdf>

- Chou, C., & Peng, H. (2011). Promoting awareness of Internet safety in Taiwan in-service teacher education: A ten-year experience. *Internet and Higher Education*, 14(1), 44–53. Retrieved on June 6, 2013 from <http://www.eric.ed.gov>
- Committee on National Security Systems. (2010, April). National information assurance (IA) glossary (CNSS instruction no. 4009). Retrieved on March 5, 2013 from [http://www.ncix.gov/publications/policy/docs/CNSSI\\_4009.pdf](http://www.ncix.gov/publications/policy/docs/CNSSI_4009.pdf)
- Cullingford, C., & Haq, N. (2009). Computers, schools and students: The effects of technology. England: Ashgate
- Creswell, J. W. Planning, Conducting and Evaluating Quantitative and Qualitative Research USA: Pearson, Publisher, 2012. Print.
- Çağiltay, K. Procedure Learning: Reigeluth's Approach [Online Website]. Retrieved on June 6, 2014 Lecture Notes Online Web site: <http://ocw.metu.edu.tr/mod/page/view.php?id=60>
- Damaševičius, R. R. (2009). Information systems development: Refactoring of learning objects for mobile learning. G.A. Papadopoulos et al. (eds.). Springer US
- Davidson, J. C., & Martellozzo, E. (2008). Protecting vulnerable young people in cyberspace from sexual abuse: Raising awareness and responding globally. *Police Practice and Research*, 9(4), 277–289. doi:10.1080/15614260802349965
- Eroğlu, E., & Yazar, D. (2013). Ortaöğretim bilgi ve iletişim teknolojisi ders kitabı (1th ed.). Yazar, A. (ed). Milli Eğitim Bakanlığı Yayınları. MEB Devlet Kitapları.
- ETPRO-NCSA. (2008). 2008 National Cyberethics, Cybersafety, Cybersecurity Baseline Study. Retrieved on June 2, 2013 from <http://www.whitehouse.gov/>
- ETPRO-NCSA. (2010). State of K12 Cyberethics, Safety and Security Curriculum in U.S.: 2010 Educator Opinion Retrieved on August 25, 2014 from <http://www.edtechpolicy.org/cyberk12/Documents/C3Awareness/2010Survey.pdf>

- Field, A. P. (2009). *Discovering statistics using IBM SPSS statistics: and sex and drugs and rock 'n' roll / Andy Field (3<sup>rd</sup> ed.)*. Los Angeles: Sage. Retrieved on June 8, 2013 from <http://hoangftu.files.wordpress.com/2014/03/andy-field-discovering-statistics-using-spss-third-edition-2009.pdf>
- Hsiao, H.-C., Tu, Y.-L., & Chung, H.-N. (2012). Perceived social supports, computer self-efficacy, and computer use among high school students. *The Turkish Online Journal of Educational Technology*, 11(2), 167-177. Retrieved on June 4, 2013 from <http://files.eric.ed.gov/fulltext/EJ989025.pdf>
- Hazari, S., Hargrave, W., & Clenney, B. (2008). An empirical investigation of factors influencing information security behavior. *Journal of Information Privacy & Security*, 4(4), 3-20.
- Hew, K. F., & Brush, T. (2007). Integrating technology into K–12 teaching and learning: Current knowledge gaps and recommendations for future research. *Educational Technology Research and Development*, 55, 223–252. Retrieved on June 13, 2014 from [http://santerzero.pbworks.com/f/Integrating%2Btechnology%2Binto%2Bk\\_12%2Bteaching.pdf](http://santerzero.pbworks.com/f/Integrating%2Btechnology%2Binto%2Bk_12%2Bteaching.pdf)
- Hentea, M. (2005) . A perspective on achieving information security awareness. *Issues in informing science and information*, 2, 169-178. Retrieved on June 13, 2012 from <http://2005papers.iisit.org/I14f89Hent.pdf>
- Hechter, R. P., & Vermette, L. (2013). Technology integration in K-12 science classrooms: An analysis of barriers and implications. *Themes In Science & Technology Education*, 6(2), 73-90.
- Hinkle, D. E., Wiersma, W., & Jurs, S. G. (2003). *Applied statistics for the behavioral sciences (5<sup>th</sup> ed.)*. Boston: Houghton Mifflin.
- Inan, F., & Lowther, D. (2010). Laptops in the K-12 classrooms: Exploring factors impacting instructional use. *Computers And Education*, 55(3), 937-944. doi:10.1016/j.compedu.2010.04.004
- Information Technology. (n.d.). In Merriam-Webster's Collegiate Dictionary *online*. Retrieved on January 5, 2014 from <http://www.merriam-webster.com/dictionary/information%20technology>

- I-TECH (2010). Guidelines for pre- and post-testing: a technical implementation guide. Retrieved on January 2, 2014 from <http://www.go2itech.org/resources/technical-implementation-guides>
- Ismail, M. A., Rahman, S., Hassan, I. S., & Mahmud, R. (2008). Web based learning through mobile technology for architectural education. Proceedings of the 7<sup>th</sup> WSEAS International Conference on Education and Educational Technology (EDU'08)
- Jones, L. M., Mitchell, K. J., & Finkelhor, D. (2012). Trends in youth internet victimization: Findings from three youth internet safety surveys 2000–2010. *Journal of Adolescent Health, 50*, 179–186
- Kabakçı, I. & Can, V. (2009). Views of computer teachers about the primary school students' safety on the computer & internet. *Çağdaş Eğitim Dergisi, 34 (361)*, 13-2
- Kaspersky. (2013, August). Kaspersky lab IT threat evolution: Q2 2013. Retrieved on June 9, 2013 from [http://www.securelist.com/en/analysis/204792299/IT\\_Threat\\_Evolution\\_Q2\\_2013](http://www.securelist.com/en/analysis/204792299/IT_Threat_Evolution_Q2_2013)
- Lantzy, J. (2009). Protecting children in cyberspace: A higher education case study. Dissertation Abstracts International Section A,70, 110.
- Lazarinis, F. (2010). Online risks obstructing safe internet access for students. *Electronic Library, 28(1)*, 157-170. doi:10.1108/02640471011023441
- Liang, H., & Xue, Y. (2009). Avoidance of information technology threats: A theoretical perspective. *MIS Quarterly, 33(1)*, 71–90. Retrieved on June 23, 2013 from <http://www.misq.org/>
- McDaniel, J. E., & Early, J. B. (2013). Internet Safety Education: Pittsylvania County Schools. Retrieved on July 15, 2014 from <http://www.pcs.k12.va.us/isafety/safety.pdf>
- Mensch, S. & Wilkie, L. (2011). Information security activities of college students: an exploratory study. *Academy of Information & Management Sciences Journal, 14(2)*, 91-116. Retrieved on June 13, 2013 from <http://www.aabri.com/>

Milli Eğitim Bakanlığı (MEB). (n.d). BT araçlarının bilinçli ve güvenli kullanımı. Retrieved on January 18, 2014 from <http://fatihprojesi.meb.gov.tr/icerikeklenti/e131211132820.pdf>

Milli Eğitim Bakanlığı (MEB). (2011a). Tablet Bilgisayar 3 Şartnamesi. Retrieved on January 18, 2014 from: <https://www.dmo.gov.tr/Duyurular/DmoIhaleDuyurulariEk/3514-2-teknik%20%C5%9Fartname.pdf>

Milli Eğitim Bakanlığı (MEB). (2011b). Bilişim teknolojileri alanı çerçeve öğretim programı. Retrieved on June 5, 2013 from [http://mebk12.meb.gov.tr/meb\\_iys\\_dosyalar/35/25/966426/dosyalar/2012\\_12/05121710\\_bc10ae0d38334ff88785a070d294f0c4.pdf](http://mebk12.meb.gov.tr/meb_iys_dosyalar/35/25/966426/dosyalar/2012_12/05121710_bc10ae0d38334ff88785a070d294f0c4.pdf)

Milli Eğitim Bakanlığı (MEB). (2004). İnternet etiği. Retrieved on January 18, 2014 from <http://www.meb.gov.tr/duyurular/duyurular/internetEtigi/intEtik.htm>

Mitnick, K. D., Simon, W. L., & Wozniak, S., (2003). Security's Weakest Link. The Art of Deception: Controlling the Human Element of Security (pp. 1-12). Indiana, Indianapolis: Wiley Publishing, Inc. Retrieved on April 5, 2013 from <http://proquestcombo.safaribooksonline.com/9780764542800>

Molenda, M. (2003). In search of the elusive ADDIE model. *Performance Improvement*, 42(5), 34–37. doi: 10.1002/pfi.4930420508

Mueller, J. (2010). Computer integration in elementary and secondary schools: Variables influencing educators. *Dissertation Abstracts International Section A*, 70, 2387.

National Cyber Security Alliance [NCSA]. (n.d.). About Us. Retrieved on June 1, 2014 from <http://www.staysafeonline.org/ncsam/about>

National Cyber Security Alliance [NCSA]. (2014). National Cyber Security Awareness Month: Over the past 10 years. Retrieved on June 6, 2013 from <https://www.staysafeonline.org/>

5651 Law No, § 4 (2007).

- Rufi, A. W. (2006). Network Security 1 and 2 Companion Guide (Cisco Networking Academy): Vulnerabilities, Threats, and Attacks. Retrieved on June 21, 2013 from <http://ptgmedia.pearsoncmg.com/images/1587131625/samplechapter/1587131625content.pdf>
- Presidency of Telecommunication. (n.d). Publications aimed awareness raising. Retrieved on June 16, 2014 from [http://www.tib.gov.tr/tr/tr-menu-70-bilinlendirme\\_amacli\\_yayinlar.html](http://www.tib.gov.tr/tr/tr-menu-70-bilinlendirme_amacli_yayinlar.html).
- Snyder, T.D., and Dillow, S.A. (2013). Digest of Education Statistics 2012 (NCES 2014-015). National Center. Retrieved on July 22, 2014 from <http://nces.ed.gov/pubs2014/2014015.pdf>
- Lieu, C. (2002). Social Engineering – Attacking the Weakest Link. Global Information Assurance Certification Paper, SANS institute, GSEC Practical Assignment, Version 1.4, Option 1. Retrieved on June 3, 2013 from <http://www.giac.org/paper/gsec/2082/social-engineering-attacking-weakest-link/103563>
- Livingstone, S., Haddon, L., Görzig, A., & Ólafsson, K. (2011). Risks and safety on the internet: The perspective of European children: Full findings. LSE, London: EU Kids Online. Retrieved on June 14, 2013 from [http://www2.cnrs.fr/sites/en/fichier/rapport\\_english.pdf](http://www2.cnrs.fr/sites/en/fichier/rapport_english.pdf)
- OECD. (2004, September). Summary of responses to the survey on the implementation of the OECD Guidelines for the security of information systems and networks: Towards a culture of security. Retrieved on January 18, 2014 from <http://www.oecd.org/sti/security-privacy>
- OECD. (2005). Are Students Ready for a Technology-Rich World? What PISA Studies Tell Us? Retrieved on January 18, 2014 from <http://www.oecd.org/>
- OECD. (2012). The Protection of Children Online: Recommendation of the OECD Council Report on risks faced by children online and policies to protect them. Retrieved on January 18, 2014 from [http://www.oecd.org/sti/ieconomy/childrenonline\\_with\\_cover.pdf](http://www.oecd.org/sti/ieconomy/childrenonline_with_cover.pdf)



- Delialiođlu, Ö. (2011). Biliřim sistemleri gvenliđi ve ilgili etik kavramlar. In A. Őentrk (Ed), *Temel bilgi teknolojileri ve bilgisayar kullanımı* (pp. 509-537). Bursa: Ekin Basım Yayın Dađıtım.
- Peng, T. K. & Ramaiah, C. K. (2007, November 6). Awareness of Cyber Laws in Young Singaporeans. *DESIDOC Bulletin of Information Technology*, 27 (6), 41-53. Retrieved on January 15, 2013 from <http://publications.drdo.gov.in>
- Peterson, C. (2003). Bringing ADDIE to life: Instructional design at its best. *Journal of Educational Multimedia and Hypermedia*. 12(3), 227-241. Retrieved on January 18, 2014 from <http://eric.ed.gov/?id=EJ822355>.
- Smith, M. (1998). Security-Who cares? *Computer Fraud & Security*, 1998 (4). 12-15. doi:10.1016/S1361-3723(97)86610-9
- Symantec Corporation. (2013, April). Internet security threat report, 2013. 18. Retrieved on January 18, 2013 from [http://www.symantec.com/security\\_response/publications/threatreport.jsp](http://www.symantec.com/security_response/publications/threatreport.jsp)
- Srum, H., Andersen, K., & Vatrapu, R. (2012). Public websites and human-computer interaction: an empirical study of measurement of website quality and user satisfaction. *Behaviour & Information Technology*, 31(7), 697-706. doi:10.1080/0144929X.2011.577191
- Thompson S. T. C. (2006). Helping the hacker? Library information, security, and social engineering. *Information Technology & Libraries*, 25 (4), 222-224. doi:10.6017/ital.v25i4.3355
- Trkiye İstatistik Kurumu (TUİK). (2012, June). *Hanehalkı Biliřim Teknolojileri Kullanım Arařtırması*. Retrieved on January 10, 2013 from [www.tuik.gov.tr](http://www.tuik.gov.tr)
- Trkiye İstatistik Kurumu (TUİK). (2013, June). *Hanehalkı Biliřim Teknolojileri Kullanım Arařtırması*. Retrieved on January 10, 2013 from [tuik.gov.tr](http://tuik.gov.tr)
- Van Teijlingen, E. R., & Hundley, V. (2001). The importance of pilot studies. *Social Research Update*, (35), 1.

- Van Teijlingen, E., Rennie, A., Hundley, V., & Graham, W. (2001). The importance of conducting and reporting pilot studies: The example of the Scottish Births Survey. *Journal Of Advanced Nursing*, 34(3), 289-295. doi:10.1046/j.1365-2648.2001.01757.x
- Valcke, M., Bonte, S., De Wever, B., & Rots, I. (2010). Internet parenting styles and the impact on Internet use of primary school children. *Computers & Education*, 55 (2), p454-464. Retrieved on February 18, 2013 from <http://www.eric.ed.gov>
- Victory, N. J. (2003). Children's Internet Protection Act.: Study of Technology Protection Measures in Section 1703. Retrieved on March 20, 2014 from <http://www.ntia.doc.gov/files/ntia/publications/cipareport08142003.pdf>
- Valcke, M., Schellens, T., Van Keer, H. & Gerarts, M. (2007). Primary school children's safe and unsafe use of the Internet at home and at school: An exploratory study. *Computers in Human Behavior*, 23(6), 2838–2850. Retrieved on February 18, 2014 from <http://www.sciencedirect.com>
- Yiğit, Y. & Yıldırım, S. & Özden, M. Y. (2000). “Web Tabanlı İnternet Öğreticisi: Bir Durum Çalışması.” Hacettepe Üniversitesi Eğitim Fakültesi Dergisi. 19, s.166-176. Retrieved on December 18, 2013 from <http://www.metu.edu.tr/~soner/NationalJournals.html>
- Wilson, M. & Hash, J. (2003). Building an Information Technology Security Awareness and Training Program: Computer Security. Washington, DC
- Wishart, J. (2004). Internet safety in emerging educational contexts. *Computers & Education*, 43 (1-2), 193–204. Retrieved on April 18, 2013 from <http://www.eric.ed.gov>

## APPENDIX A

### FINAL VERSION OF PKSOITS-1 (INTURKISH)

Değerli Katılımcılar.

Bu çalışmanın amacı Türkiye’de orta dereceli okullarda bulunan öğrencilerin günden güne yaygınlaşan bilişim teknolojileri araçlarının güvenli kullanımı hakkındaki farkındalık ve beceri düzeyleri ile öğretmenlerin bu bilgi ve beceri düzeyine etkisini belirlemektir. Lütfen aşağıdaki sorularda size en uygun olan seçeneği/seçenekleri işaretleyiniz.

#### I. Genel Sorular

1. Kullanıcı adı (Anketi doldurduktan 1 gün sonra [www.bilinlibirey.com](http://www.bilinlibirey.com) isimli web sitesi kullanımınıza açılacaktır. Kullanıcı adı ve şifreniz burada belirlediğiniz kullanıcı adınız olacaktır.):

\_\_\_\_\_

2. Cinsiyetiniz

Kadın  Erkek

3. Yaşınız: \_\_\_\_\_

4. Okulunuz ve Sınıfınız: \_\_\_\_\_

5. Aşağıdaki bilişim cihazlarından hangilerini kullanıyorsunuz? (Birden fazla seçeneği işaretleyebilirsiniz.)

Kendime ait bilgisayar kullanıyorum (masaüstü veya dizüstü)

Ailenin ortak kullanımında olan bilgisayar kullanıyorum (masaüstü veya dizüstü)

Bilgisayar laboratuvarlarındaki ait olan bilgisayar kullanıyorum (masaüstü bilgisayar. dizüstü)

- Tablet bilgisayar kullanıyorum
- Akıllı telefon kullanıyorum
- Diğer (Belirtiniz).....

*Günde ortalama kaç saat bilgisayar kullanıyorsunuz?*

- 0-1 saat
- 1-3 saat
- 3 saatten daha fazla

*İnterneti en çok hangi amaç için kullanıyorsunuz? (Lütfen sadece bir seçenek işaretleyiniz.)*

- Araştırma
- Zaman geçirmek
- İletişim kurmak
- İş amaçlı
- Diğer (Belirtiniz).....
- Ders çalışmak/ödev yapmak

*İnternete aşağıdaki araçlardan hangisi ile bağlanıyorsunuz? (Birden fazla seçeneği işaretleyebilirsiniz.)*

- Masaüstü bilgisayar
- Dizüstü bilgisayar (Laptop)
- Tablet bilgisayar
- Telefon
- Diğer (Belirtiniz).....

6. Aşağıdaki işletim sistemlerinden hangisini/hangilerini kullanıyorsunuz? (Birden fazla seçeneği işaretleyebilirsiniz.)

- Kullanmıyorum
- Windows
- Mac OS X
- iOS
- Android
- Linux
- Diğer (Belirtiniz):.....

7. Aşağıdaki Sosyal Paylaşım Sitelerinden hangisini/hangilerini kullanıyorsunuz? (Birden fazla seçeneği işaretleyebilirsiniz.)

- Kullanmıyorum
- Facebook
- Twitter
- Diğer (Belirtiniz):.....

*Bilgisayarınızda lisanssız yazılım (program) var mı?*

- Evet
- Hayır

*İnternette müzik, film, oyun dosyaları indiriyor musunuz?*

- Evet
- Hayır

*Evde interneti kullanma saatleri var mı?*

- Evet
- Hayır

8. En sık kullandığınız web tarayıcısı hangisidir? (En fazla iki seçeneği işaretleyiniz.)
- Kullanmıyorum  Internet Explorer  Google Chrome  
 Mozilla Firefox  Apple Safari  
 Diğer (Belirtiniz):.....

*Aşağıdaki kavramlardan hangisini/hangilerini daha önce duydunuz? (Birden fazla seçeneği işaretleyebilirsiniz.)*

- Virüs  
 Saldırı  
 Tehdit  
 Risk  
 Sistem açığı (Sistem Boşluğu)  
 Saldırgan (Hacker)

*Size göre aşağıdaki bilişim suçlarından en tehlikelisi hangisidir? (Lütfen sadece 1 (bir) seçenek işaretleyiniz)*

- Lisanssız ürün kullanmak  
 Dolandırıcılık (ATM. kredi kartı vb.)  
 Yasa dışı yayınlar (pornografik. hakaret)  
 Bilgisayarın izinsiz kullanımı  
 Diğer (Belirtiniz).....

*Aşağıdaki bilişim suçlarından herhangi birine maruz kaldınız mı? (Birden fazla seçeneği işaretleyebilirsiniz.)*

- Bilgisayara virüs bulaşması  
 İstenmeyen fotoğrafların görüntülenmesine maruz kalmak (pornografik)  
 İftira  
 Bilgisayar sistemi üzerinden yetkisiz kontrol/erişim  
 Sahtekârlık (kimlik. banka bilgilerinin çalınması gibi)  
 Herhangi bir bilişim suçuna maruz kalmadım  
 Diğer (Belirtiniz).....

9. Aşağıdaki e-posta servislerinden hangisi/hangilerini kullanıyorsunuz? (En fazla iki seçeneği işaretleyiniz.)

- Kullanmıyorum  Hotmail  Gmail  
 Yahoo  Diğer (Belirtiniz):.....

## **II. Bilgi Güvenliği Bilgi Seviyesi/Farkındalığıyla ilgili Sorular**

10. Aşağıdakilerden hangisi virüslerin (zararlı yazımların) bilişim cihazlarına bulaşmasına sebep olabilecek en doğru tanımı içermektedir? (Lütfen sadece **bir** seçenek işaretleyiniz.)

- Sadece internete bağlanması sonucu bulaşırlar.  
 Sadece herhangi bir güvenlik önlemi almadan internete bağlanması sonucu bulaşırlar.

- Herhangi bir güvenlik önlemi almadan internetten dosya indirilmesi. CD. DVD. Flash bellek gibi cihazlardan dosya aktarılması ile bulaşırlar.
- Sadece kablolu internet bağlantısı ile bulaşırlar.
- Sadece kablosuz internet bağlantısı ile bulaşırlar.
- Bilmiyorum.

11. Zararlı yazılımları (virüsleri) engellemek için kişisel bilgisayarlarınızda aşağıdaki yöntemlerden hangilerini kullanıyorsunuz? (Birden fazla seçeneği işaretleyebilirsiniz.)

- Herhangi bir yöntem kullanmıyorum.
- Anti virüs
- Anti-Spyware/Adware
- Şifre
- Sertifika
- Yazılım güncellemesi
- Güvenlik duvarı
- Diğer (Belirtiniz):.....

*Okulunuzda bilgisayar ve internet kullanımı ile ilgili yazılı kurallar var mı?*

- Evet
- Hayır

*Evde bilgisayar ve internet kullanımı ile ilgili yazılı kurallar var mı?*

- Evet
- Hayır

12. Okulunuza bilgisayar ve internet kullanımı ile ilgili yazılı kurallar varsa aşağıdakilerden hangilerini içermektedir? (Birden fazla seçeneği işaretleyebilirsiniz.)

- Okulumuzda bilgisayar ve internet kullanımı ile ilgili yazılı kurallar bulunmamaktadır.
- Okul bilgisayarının nasıl ve hangi amaçlarla kullanılabilceği belirlenmiştir.
- Okul internetinin ne amaçla kullanılabilceği belirlenmiştir.
- Bilgisayar ile ilgili sorunlar yaşandığında kiminle iletişime geçilmesi gerektiği belirlenmiştir.
- Diğer (Belirtiniz):.....

13. Evinizde bilgisayar ve internet kullanımı ile ilgili yazılı/sözlü kurallar varsa aşağıdakilerden hangilerini içermektedir? (Birden fazla seçeneği işaretleyebilirsiniz.)

- Evinizde bilgisayar ve internet kullanımı ile ilgili kurallar bulunmamaktadır.
- Bilgisayarın günlük kullanım saatini belirleyen kural vardır.
- Bilgisayara izinsiz internetten. CD. DVD veya Flash bellekten herhangi bir dosya yüklenmemesiyle ilgili kural vardır.
- İnternet üzerinden yabancılarla konuşulmamasıyla ilgili kural vardır.
- Adı. soyadı. yaş. telefon. adres gibi kişisel bilgilerin internet üzerinden paylaşılmaması ile ilgili kural vardır.

- ( ) Yabancılardan gelen e-postaların açılmaması ile ilgili kural vardır.
- ( ) İnternetteki tutum ve davranışların nasıl olacağı ile kural vardır.
- ( ) Bilgisayara izinsiz program kurulmaması ile kural vardır.
- ( ) Sadece onay verilen web sitelerine girilmesi ile kural vardır.
- ( ) Diğer (Belirtiniz):.....

**Aşağıda verilen sorular Bilgi Teknolojileri (BT) cihazlarının ne derece güvenli kullanıldığını belirlemek amacıyla hazırlanmıştır. Lütfen her soruyu dikkatlice okuyunuz ve size en uygun düzeyi işaretleyiniz.**

**Bölüm 1:**

**Bilgi ve Bilgilendirilme**

1: Hiç. 2: Biraz. 3:Orta. 4:İyi. 5: Çok İyi

|  | 1 | 2 | 3 | 4 | 5 |
|--|---|---|---|---|---|
| 14. Bilişim suçlarıyla ilgili bilgi düzeyiniz ne nedir?  |   |   |   |   |   |
| 15. Bilişim suçları karşısında neler yapılabileceğiniz konusunda bilgi düzeyiniz nedir?          |   |   |   |   |   |
| 16. Lisanssız yazılımların zararları hakkındaki bilgi düzeyiniz nedir?                           |   |   |   |   |   |
| 17. Lisanssız yazılım kullanımının cezai sorumlulukları konusunda bilgi seviyeniz ne düzeydedir? |   |   |   |   |   |
| 18. Aileniz sizi bilgi güvenliği konusunda ne düzeyde bilgilendiriyor?                           |   |   |   |   |   |
| 19. Okulunuzda bilgi güvenliği konusunda ne düzeyde bilgilendirme yapılıyor?                     |   |   |   |   |   |
| 20. Sınıfta güvenli bilgisayar kullanımı konusunda ne düzeyde bilgilendiriliyorsunuz?            |   |   |   |   |   |

**Bölüm 2:**

*Okulunuzda bilgisayar ve internet kullanımı ile ilgili yazılı kurallar yoksa Bölüm 3'e geçiniz.*

1: Hiç. 2: Biraz. 3:-Orta. 4:İyi. 5: Çok İyi

|  | 1 | 2 | 3 | 4 | 5 |
|--|---|---|---|---|---|
| 21. Bu yazılı kurallar hakkında ne düzeyde bilgilendirildiniz?                             |   |   |   |   |   |
| 22. Bu yazılı kurallara ne kadar kolay ulaşabilmektesiniz?                                 |   |   |   |   |   |
| 23. Kullanım kuralları ne düzeyde anlaşılır yazılmıştır?                                   |   |   |   |   |   |
| 24. Bilgisayar ve internet kullanımı ile ilgili kurallar ne düzeyde anlaşılır yazılmıştır? |   |   |   |   |   |

**III. Bilgi Teknolojilerinin Güvenli Kullanım Bilgisi**

**Bölüm 3:**

1:Hiç. 2: Biraz; 3:Orta; 4: İyi; 5:Çok İyi

|  | 1 | 2 | 3 | 4 | 5 |
|--|---|---|---|---|---|
|  |   |   |   |   |   |

|   |  |  |  |  |  |
|---|--|--|--|--|--|
| 25. Bilgi güvenliğinin sağlanması konusunda bilgi seviyeniz nedir?                                      |  |  |  |  |  |
| 26. Kullandığınız işletim sisteminin ekran koruyucusunun şifrelenmesi hakkındaki bilgi düzeyiniz nedir? |  |  |  |  |  |
| 27. Kullanıcı hesapları oluşturulması hakkındaki bilgi düzeyiniz nedir?                                 |  |  |  |  |  |
| 28. Kullandığınız işletim sisteminin şifrelenmesi hakkındaki bilgi düzeyiniz nedir?                     |  |  |  |  |  |
| 29. Kullandığınız işletim sisteminin güncellenmesi hakkındaki bilgi düzeyiniz nedir?                    |  |  |  |  |  |

#### Bölüm 4:

*Windows işletim sistemi kullanmıyorsanız Bölüm 5'e geçiniz.*

1:Hiç; 2:Az; 3:Orta; 4: İyi; 5:Çok İyi

|   | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| 30. Güvenlik Duvarı hakkındaki bilgi düzeyiniz nedir? |   |   |   |   |   |
| 31. Defender hakkındaki bilgi düzeyiniz nedir?        |   |   |   |   |   |

#### Bölüm 5:

*MAC OS işletim sistemi kullanmıyorsanız Bölüm 6'ya geçiniz.*

1:Hiç; 2:Az; 3:Orta; 4: İyi; 5:Çok İyi

|   | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| 32. Sandbox hakkındaki bilgi düzeyiniz nedir?   |   |   |   |   |   |
| 33. FileVault hakkındaki bilgi düzeyiniz nedir?   |   |   |   |   |   |
| 34. Güvenlik ve Gizlilik Penceresi (Security and Privacy) hakkındaki bilgi düzeyiniz nedir? |   |   |   |   |   |
| 35. Finding missing MAC hakkındaki bilgi düzeyiniz nedir?                                   |   |   |   |   |   |
| <i>Antipishing hakkındaki bilgi seviyeniz nedir?</i>  |   |   |   |   |   |
| 36. Password Assistant hakkındaki bilgi düzeyiniz nedir?                                    |   |   |   |   |   |
| <i>SecureEmptyTrash hakkındaki bilgi seviyeniz nedir?</i>                                   |   |   |   |   |   |

#### Bölüm 6:

*Android işletim sistemi kullanmıyorsanız Bölüm 7'ye geçiniz.*

1:Hiç; 2:Az; 3:Orta; 4: İyi; 5:Çok İyi

|  | 1 | 2 | 3 | 4 | 5 |
|--|---|---|---|---|---|
| <i>Üçüncü Parti uygulamalar hakkındaki bilgi seviyeniz nedir?</i>                            |   |   |   |   |   |
| <i>Kişisel Bilgilerin (Personal Information) korunması hakkındaki bilgi seviyeniz nedir?</i> |   |   |   |   |   |
| 37. Ayarlar Menüsü hakkındaki bilgi düzeyiniz nedir?   |   |   |   |   |   |
| 38. Ekran kilidi hakkındaki bilgi düzeyiniz nedir?   |   |   |   |   |   |
| 39. Sahip bilgileri eklenmesi hakkında bilgi düzeyiniz nedir?                                |   |   |   |   |   |



**Bölüm 7:**

E-posta kullanmıyorsanız Bölüm 8'e geçiniz.

1:Hiçbir zaman. 2:Bazen; 3:Kararsızım; 4: Genellikle; 5:Her zaman

|  | 1 | 2 | 3 | 4 | 5 |
|--|---|---|---|---|---|
| 40. Tanımadığınız kişilerden gelen e-postları ne sıklıkla açarsınız?   |   |   |   |   |   |
| 41. Tanımadığınız kişilerden e-posta ile gelen linklere ne sıklıkla tıklarsınız?                                 |   |   |   |   |   |
| 42. Tanımadığınız kişilerden e-posta ile gelen ekleri ne sıklıkla açarsınız?                                     |   |   |   |   |   |
| 43. Kullandığınız e-posta programının (Hotmail. Gmail. Yahoovb) filtrelenmesi konusundaki bilgi düzeyiniz nedir? |   |   |   |   |   |

**Bölüm 8:****İnternetin Güvenli Kullanımı**

1:Hiç. 2:Biraz; 3:Orta; 4: İyi; 5:Çok İyi

|   | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| 44. En sık kullandığınız tarayıcının güvenlik ayarları hakkındaki bilgi düzeyiniz nedir?          |   |   |   |   |   |
| 45. Sosyal ağlar üzerinden kişisel bilgi paylaşımının zararları hakkındaki bilgi düzeyiniz nedir? |   |   |   |   |   |
| 46. Kullandığınız sosyal ağların güvenlik-gizlilik ayarları hakkındaki bilgi düzeyiniz nedir?     |   |   |   |   |   |



## APPENDIX B

### FINAL VERSION OF PKSOITS-2 (INTURKISH)

Değerli Katılımcılar.

Bu çalışmanın amacı Türkiye’de orta dereceli okullarda bulunan öğrencilerin günden güne yaygınlaşan bilişim teknolojileri araçlarının güvenli kullanımı hakkındaki farkındalık ve beceri düzeyleri ile öğretmenlerin bu bilgi ve beceri düzeyine etkisini belirlemektir. Lütfen aşağıdaki sorularda size en uygun olan seçeneği/seçenekleri işaretleyiniz.

#### I. Genel Sorular

1. Kullanıcı adı (Lütfen birinci ankette kullandığımız kullanıcı adınızı yazınız.):

\_\_\_\_\_

2. Okulunuz ve Sınıfınız: \_\_\_\_\_

#### II. Bilgi Güvenliği Bilgi Seviyesi/Farkındalığıyla ilgili Sorular

3. Aşağıdakilerden hangisi virüslerin (zararlı yazımların) bilişim cihazlarına bulaşmasına sebep olabilecek en doğru tanımı içermektedir? (Lütfen sadece **bir** seçenek işaretleyiniz.)

- Sadece internete bağlanması sonucu bulaşırlar.
- Sadece herhangi bir güvenlik önlemi almadan internete bağlanması sonucu bulaşırlar.
- Herhangi bir güvenlik önlemi almadan internetten dosya indirilmesi. CD. DVD. Flash bellek gibi cihazlardan dosya aktarılması ile bulaşırlar.
- Sadece kablolu internet bağlantısı ile bulaşırlar.
- Sadece kablosuz internet bağlantısı ile bulaşırlar.
- Bilmiyorum.

4. Zararlı yazılımları (virüsleri) engellemek için kişisel bilgisayarlarınızda aşağıdaki yöntemlerden hangilerini kullanıyorsunuz? (Birden fazla seçeneği işaretleyebilirsiniz.)

- ( ) Herhangi bir yöntem kullanmıyorum  
 .  
 ( ) Anti virüs  
 ( ) Anti-Spyware/Adware ( ) Şifre  
 ( ) Sertifika  
 ( ) Yazılım güncellemesi  
 ( ) Güvenlik duvarı  
 ( ) Diğer (Belirtiniz):.....

Aşağıda verilen sorular Bilgi Teknolojileri (BT) cihazlarının ne derece güvenli kullanıldığını belirlemek amacıyla hazırlanmıştır. Lütfen her soruyu dikkatlice okuyunuz ve size en uygun düzeyi işaretleyiniz.

**Bölüm 1:**

**Bilgi ve Bilgilendirilme**

1: Hiç. 2: Biraz. 3:Orta. 4:İyi. 5: Çok İyi

|  | 1 | 2 | 3 | 4 | 5 |
|--|---|---|---|---|---|
| 5. Bilişim suçlarıyla ilgili bilgi düzeyiniz ne nedir?   |   |   |   |   |   |
| 6. Bilişim suçları karşısında neler yapılabileceğiniz konusunda bilgi düzeyiniz nedir?         |   |   |   |   |   |
| 7. Lisanssız yazılımların zararları hakkındaki bilgi düzeyiniz nedir?                          |   |   |   |   |   |
| 8. Lisansız yazılım kullanımının cezai sorumlulukları konusunda bilgi seviyeniz ne düzeydedir? |   |   |   |   |   |

**III. Bilgi Teknolojilerinin Güvenli Kullanım Bilgisi**

**Bölüm 3:**

1:Hiç. 2: Biraz; 3:Orta; 4: İyi; 5:Çok İyi

|  | 1 | 2 | 3 | 4 | 5 |
|--|---|---|---|---|---|
| 9. Kullandığınız işletim sisteminin ekran koruyucusunun şifrenmesi hakkındaki bilgi düzeyiniz nedir? |   |   |   |   |   |
| 10. Kullanıcı hesapları oluşturulması hakkındaki bilgi düzeyiniz nedir?                              |   |   |   |   |   |
| 11. Kullandığınız işletim sisteminin şifrenmesi hakkındaki bilgi düzeyiniz nedir?                    |   |   |   |   |   |
| 12. Kullandığınız işletim sisteminin güncellenmesi hakkındaki bilgi düzeyiniz nedir?                 |   |   |   |   |   |

**Bölüm 4:**

*Windows işletim sistemi kullanmıyorsanız Bölüm 5'e geçiniz.*

1:Hiç. 2: Biraz; 3:Orta; 4: İyi; 5:Çok İyi

|   | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| 13. Güvenlik Duvarı hakkındaki bilgi düzeyiniz nedir? |   |   |   |   |   |

|  |  |  |  |  |  |
|--|--|--|--|--|--|
| 14. Defender hakkındaki bilgi düzeyiniz nedir? |  |  |  |  |  |
|--|--|--|--|--|--|

**Bölüm 5:**

MAC OS işletim sistemi kullanmıyorsanız Bölüm 6'ya geçiniz.

|   | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| 15. Sandbox hakkındaki bilgi düzeyiniz nedir?   |   |   |   |   |   |
| 16. FileVault hakkındaki bilgi düzeyiniz nedir?   |   |   |   |   |   |
| 17. Güvenlik ve Gizlilik Penceresi (Security and Privacy) hakkındaki bilgi düzeyiniz nedir? |   |   |   |   |   |
| 18. Findingmissing MAC hakkındaki bilgi düzeyiniz nedir?                                    |   |   |   |   |   |
| 19. PasswordAssistant hakkındaki bilgi düzeyiniz nedir?                                     |   |   |   |   |   |

**Bölüm 6:**

Android işletim sistemi kullanmıyorsanız Bölüm 7'ye geçiniz.

1:Hiç; 2: Biraz; 3:Orta; 4: İyi; 5:Çok İyi

|   | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| 20. Ayarlar Menüsü hakkındaki bilgi düzeyiniz nedir?          |   |   |   |   |   |
| 21. Ekran kilidi hakkındaki bilgi düzeyiniz nedir?            |   |   |   |   |   |
| 22. Sahip bilgileri eklenmesi hakkında bilgi düzeyiniz nedir? |   |   |   |   |   |

**Bölüm 7:**

E-posta kullanmıyorsanız Bölüm 8'e geçiniz.

1:Hiçbir zaman. 2:Bazen; 3:Kararsızım; 4: Genellikle; 5:Her zaman

|  | 1 | 2 | 3 | 4 | 5 |
|--|---|---|---|---|---|
| 23. Tanımadığınız kişilerden gelen e-postaları ne sıklıkla açarsınız?  |   |   |   |   |   |
| 24. Tanımadığınız kişilerden e-posta ile gelen linklere ne sıklıkla tıklarsınız?                               |   |   |   |   |   |
| 25. Tanımadığınız kişilerden e-posta ile gelen ekleri ne sıklıkla açarsınız?                                   |   |   |   |   |   |
| 26. Kullandığınız e-posta programının (Hotmail. Gmail. Yahoovb) filtrenmesi konusundaki bilgi düzeyiniz nedir? |   |   |   |   |   |

**Bölüm 8:**

**İnternetin Güvenli Kullanımı**

1:Hiç; 2: Biraz; 3:Orta; 4: İyi; 5:Çok İyi

|   | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| 27. En sık kullandığımız tarayıcının güvenlik ayarları hakkındaki bilgi düzeyiniz nedir?          |   |   |   |   |   |
| 28. Sosyal ağlar üzerinden kişisel bilgi paylaşımının zararları hakkındaki bilgi düzeyiniz nedir? |   |   |   |   |   |
| 29. Kullandığımız sosyal ağların güvenlik-gizlilik ayarları hakkındaki bilgi düzeyiniz nedir?     |   |   |   |   |   |

#### IV. Bilinçli Birey Portal Memnuniyeti

Bu bölümün soruları [www.bilinclibirey.com](http://www.bilinclibirey.com) portalına yönelik memnuniyetinizin belirlenmesi amacıyla oluşturulmuştur. Bilinçli Birey portalını kullanmadıysanız lütfen bu bölümü geçiniz. Bilinçli Birey ismi sorularda portal olarak kullanılmıştır. Lütfen sorularda size en uygun seçeneği işaretleyiniz.

1: Kesinlikle katılmıyorum    2: Katılmıyorum    3: Kısmen katılıyorum  
4: Katılıyorum    5: Kesinlikle katılıyorum

|  | 1 | 2 | 3 | 4 | 5 |
|--|---|---|---|---|---|
| 30. Portalda bulunan videoların ve makalelerin amacı net bir şekilde açıklanmıştır.                      |   |   |   |   |   |
| 31. Portalda yer alan bilgiler öğreticidir.  |   |   |   |   |   |
| 32. Portalda yer alan bilgiler günceldir   |   |   |   |   |   |
| 33. Portalda yer alan bilgiler konuyu öğretmek için yeterli düzeydedir.                                  |   |   |   |   |   |
| 34. Portalda yer alan içerik (konular) anlaşılır tasarlanmıştır.   |   |   |   |   |   |
| 35. Portalda yer alan içerik (konular) akıcı tasarlanmıştır.   |   |   |   |   |   |
| 36. Portalda yer alan bilgileri kullanarak bilişim cihazlarının güvenlik ayarlarını kolayca yapılabilir. |   |   |   |   |   |
| 37. Portalda yer alan içerik (konular) uygun yöntemler kullanılarak (video, makale) anlatılmıştır.       |   |   |   |   |   |
| 38. Portalı kullanmayı öğrenmek kolaydır.  |   |   |   |   |   |
| 39. Portal tüm konulara istenildiği an erişilebilir yapıda tasarlanmıştır.                               |   |   |   |   |   |
| 40. Portalda yer alan renkler iyi seçilmiştir ve gözü yormamaktadır.                                     |   |   |   |   |   |
| 41. Portal kullanımı kolaydır.   |   |   |   |   |   |
| 42. Portal görsel olarak iyi tasarlanmıştır.   |   |   |   |   |   |
| 43. Portaldaki video ve yazılar yeterince hızlı yüklenmektedir.  |   |   |   |   |   |
| 44. Portaldaki bağlantılar (linklerin) sorunsuz çalışmaktadır.   |   |   |   |   |   |

45. Lütfen portal ile ilgili düşüncelerinizi aşağıdaki alana yazınız:

---

## APPENDIX C

### TABLE OF SPECIFICATION (TOS) (IN TURKISH)

Table C.1 Table of specification (TOS) (in Turkish)

| İçerik   | Portal Konum  | Soru Numarası |
|--|---|---------------|
| <b>Genel Bilgi</b>   |   |               |
| Zararlı yazılardan korunma yöntemi   | Bilgilenelim>Genel Bilgi>Bilişim Terimleri/Bilgi Güvenliği                        | 11            |
| Zararlı yazılımların (virüslerin) bilgisayara nasıl bulaştığı hakkındaki bilgi       | Bilgilenelim>Genel Bilgi>Bilişim Terimleri/Bilgi Güvenliği                        | 10            |
| <b>IT Kullanımı Bilgilendirilme Oranı</b>  |   |               |
| Okulda bulunan kuralların içeriği  | Bilgilenelim>Genel Bilgi>Politikalar  | 21-24         |
| <b>Bilgi ve Bilgilendirme</b>  |   |               |
| Bilişim suçu kavramı hakkındaki bilgi düzeyi   | Bilgilenelim>Genel Bilgi>Bilişim Suçu Nedir? Yaptırımları ve Yapılması Gerekenler | 14            |
| Bilişim suçuna maruz kalındığında yapılabilecekler hakkındaki bilgi düzeyi           | Bilgilenelim>Genel Bilgi>Bilgi Güvenliği  | 15            |
| Lisanssız kullanılan yazılımlar ile ilgili cezai yaptırımlar hakkındaki bilgi düzeyi | Bilgilenelim>Genel Bilgi>Bilişim Suçu Nedir? Yaptırımları ve Yapılması Gerekenler | 17            |
| Lisanssız kullanılan yazılımların zararları hakkındaki bilgi seviyesi                | Bilgilenelim>Genel Bilgi>Bilişim Suçu Nedir? Yaptırımları ve Yapılması Gerekenler | 16            |
| <b>Windows</b>   |   |               |

|  |  |    |
|--|--|----|
| Güvenlik Duvarı hakkındaki bilgi düzeyi                            | Bilgilenelim>Genel Bilgi>Güvenlik Duvarı (Firewall)<br>Video-Animasyon>Windows>Windows Güvenlik Duvarı (Firewall)  | 29 |
| Defender hakkındaki bilgi düzeyi                                   | Bilgilenelim >Windows>Defender   | 30 |
| Ekran koruyucunun şifrelenmesi                                     | Video-Animasyon>Windows>Ekran Koruyucuya Şifre Eklenmesi   | 25 |
| Kullanıcı hesabının şifrelenmesi hakkındaki bilgi seviyesi         | Bilgilenelim>Windows>Windows Kullanıcı Hesabı Eklenmesi<br>Video-Animasyon>Windows>Windows Kullanıcı Hesabı Şifresinin Değiştirilmesi<br>Bilgilenelim>Windows>Windows Açılışa Şifre Nasıl Eklenir? | 27 |
| İşletim sisteminin güncellenmesi hakkındaki bilgi seviyesi         | Video-Animasyon>Windows>İşletim Sisteminin Güncellenmesi   | 28 |
| <b>MAC</b>   |  |    |
| Sandbox hakkındaki bilgi düzeyi                                    | Bilgilenelim>MAC>Sandboxing  | 31 |
| FileVault hakkındaki bilgi düzeyi                                  | Bilgilenelim>MAC>Dosyaların Kriptolanması (FileValut)  | 32 |
| Security & Privacy Window hakkındaki bilgi düzeyi                  | Bilgilenelim>MAC>Menu içindeki bilgiler bu pencere ile ilgilidir.  | 33 |
| Finding Missing MAC hakkındaki bilgi düzeyi                        | Bilgilenelim>MAC>Finding Missing MAC   | 34 |
| Password Assistant hakkındaki bilgi düzeyi                         | Bilgilenelim>MAC>Password Assistant  | 35 |
| Kullanıcı hesabının şifrelenmesi hakkındaki bilgi seviyeniz nedir? | Bilgilenelim>MAC> Güvenlik Penceresi-Genel Tabı (yazıldı-görsellerden sonra eklenecek)   | 27 |
| <b>Android</b>   |  |    |
| Ayarlar (Settings) menüsü hakkındaki bilgi düzeyi                  | Bilgilenelim>Android>Tablete Şifre Eklenmesi<br>Bilgilenelim>Android>Kablosuz İnternetin ve Bluetooth'un Ayarlanması   | 36 |
| Kişisel bilgilerin korunması hakkındaki bilgi düzeyi               | Bilgilenelim>Android>Tablete Şifre Eklenmesi   | 37 |



|   |   |    |
|---|---|----|
| Kullanıcı bilgileri notu ekleme   | Bilgilenelim>Android>Tablete Şifre Eklenmesi  | 38 |
| <b>İnternetin Güvenli Kullanımı</b>   |   |    |
| Kullanılan tarayıcı hakkındaki bilgi düzeyi                                     | Bilgilenelim>Android>Tarayıcı güvenliği   | 43 |
| Sosyal ağlarda kişisel bilgilerin paylaşımının riskleri hakkındaki bilgi düzeyi | Bilgilenelim>Sosyal Paylaşım Siteleri>Facebook &Twitter Gizlilik Ayarları Nasıl Yapılır?  | 44 |
| Sosyal ağların güvenlik ayarları hakkındaki bilgi seviyesi                      | Bilgilenelim>Sosyal Paylaşım Siteleri>Arayüz Tanıtımı<br>Bilgilenelim>Sosyal Paylaşım Siteleri>Facebook &Twitter Gizlilik Ayarları Nasıl Yapılır?<br>Bilgilenelim>Sosyal Paylaşım Siteleri>Facebook Şifresi Nasıl Değiştirilir?<br>Bilgilenelim>Sosyal Paylaşım Siteleri>Twitter Şifresi Nasıl Değiştirilir?<br>Video-Animasyon>Windows>Facebook Şifre ve Gizlilik Ayarları | 45 |
| <b>E-posta kullanımı</b>  |   |    |
| Göndereni bilinmeyen/tanınmayan kişilerden gelen e-postaların açılması          | Bilgilenelim>İnternet Güvenliği>E-postanın Doğru Kullanımı<br>Bilgilenelim>Genel Bilgi>Bilgi Güvenliği  | 39 |
| Göndereni bilinmeyen/tanınmayan kişilerden gelen linklerin açılması             | Bilgilenelim>İnternet Güvenliği>E-postanın Doğru Kullanımı<br>Bilgilenelim>Genel Bilgi>Bilgi Güvenliği  | 40 |
| Göndereni bilinmeyen/tanınmayan kişilerden gelen eklerin açılması               | Bilgilenelim>İnternet Güvenliği>E-postanın Doğru Kullanımı<br>Bilgilenelim>Genel Bilgi>Bilgi Güvenliği  | 41 |
| E-posta filtrelenmesi hakkındaki bilgi seviyesi                                 | Video/Animasyon>E-posta Güvenliği>Hotmail E-posta Engelleme<br>Video/Animasyon>E-posta Güvenliği>Gmail E-posta Filtreleme   | 42 |

|   |  |
|---|--|
| E-posta şifrelerinin değiştirilmesi hakkındaki bilgi düzeyi | Bilgilenelim>İnternet Güvenliği>E-posta şifresinin güncellenmesi (Gmail)<br>Bilgilenelim>İnternet Güvenliği>E-posta şifresinin güncellenmesi (Hotmail)<br>Video/Animasyon>E-posta Güvenliği>Gmail Şifre Güncelleme<br>Video/Animasyon>E-posta Güvenliği>Hotmail Şifre ve Gizlilik Ayarları |
|---|--|

## APPENDIX D

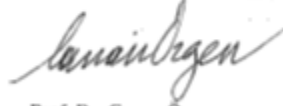
### APPROVAL WAS TAKEN FROM ETHICS COMMITTEE OF METU RESEARCH CENTER FOR APPLIED ETHICS

O.D.T.Ü  
FEN BİLİMLERİ ENSTİTÜSÜ  
YÖNETİM KURULU KARARI

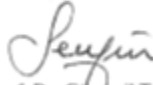
Tarih: 13.09.2012  
Sayı: FBE: 2012/ 17

#### GÖREVLENDİRME VE İZİN

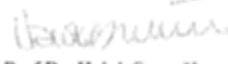
Bilgisayar ve Öğretim Teknolojileri Eğitimi EABD yüksek lisans öğrencisi Nilay Pancar'ın 15 Eylül 2012-28 Şubat 2013 tarihleri arasında "Öğrencilerin bilgi teknolojileri güvenliği alanındaki bilgi ve beceri düzeylerinin geliştirilmesinde güvenlik portalının etkisi" başlıklı araştırmasına ilişkin hazırlanan anketi, ekli etik komite başvuru formunda belirtilen okullarda uygulama yapmak için görevlendirilme başvurusu incelenmiş; ilgili danışman görüşüne dayanarak adı geçen öğrencinin isteği doğrultusunda görevlendirilmesine oybirliği ile karar verilmiştir.



Prof. Dr. Canan Özgen  
FBE Müdürü



Prof. Dr. Gürçevit Turan  
FBE Müd. Yard.



Prof. Dr. Haluk Sucuoğlu  
Üye

Prof. Dr. Zeki Kaya  
Üye



Y. Doç. Dr. Bugra Koku  
Üye



## APPENDIX E

### PERMISSION WAS TAKEN FROM MINISTRY OF TURKISH MINISTRY OF NATIONAL EDUCATION (MONE)



T.C.  
**MİLLÎ EĞİTİM BAKANLIĞI**  
Yenilik ve Eğitim Teknolojileri Genel Müdürlüğü

ÖĞRENCİ İŞLERİ  
DAİRESİ BAŞKANLIĞI  
Ev/Arg. Md. Saat :

Sayı : 81576613/44/209478  
Konu: Araştırma İzini

10/12/2012

**ORTA DOĞU TEKNİK ÜNİVERSİTESİ**  
(Öğrenci İşleri Daire Başkanlığı)

İlgi : B.30.2.ODT.72.00.00/400-51162 sayı ve 26-09-2012 tarihli yazısı

Üniversiteniz Bilgisayar ve Öğretim Lisans programı öğrencisi Nilay PANCAR'ın 15 Eylül- 28 Şubat tarihleri arasında "Öğrencilerin Bilgi Teknolojileri Alanındaki Bilgi ve Beceri Düzeylerinin Geliştirilmesinde Güvenlik Portalının Etkisi" isimli araştırmasında kullanılacak veri toplama araçlarını Ankara, Hatay, Diyarbakır, Mersin, İstanbul, Yozgat illerindeki Bakanlığımıza bağlı ortaöğretim okullarında uygulanmasına yönelik ilgi izin talebi incelenmiştir.

Üniversiteniz tarafından kabul edilerek onaylı bir örneği Bakanlığımızda muhafaza edilen veri toplama araçlarının, gönüllülük esası olmak kaydıyla, Bakanlığımıza bağlı ortaöğretim okullarında uygulanmasında bir sakınca görülmemektedir.

Bilgilerinizi ve gereğini rica ederim.

Mustafa KOÇ  
Bakan a.  
Genel Müdür

**12.12.12•019964**

10  
21.12.2012  
Ash He Ayndir  
Güvenli Elektronik İmza

Bu belge, 5070 sayılı Elektronik İmza Kanununun 5 inci maddesi gereğince güvenli elektronik imza ile imzalanmıştır



## APPENDIX F

### WILCOXON SIGNED RANKS TEST ANALYSIS RESULTS

Table F.1 Wilcoxon signed ranks test analysis results

| Item#   | Pretest-Posttest | N   | R (mean rank) | Z      | p    |
|---|------------------|-----|---------------|--------|------|
| Perceived knowledge level of the participants on virus infections (Q10) | Negative Ranks   | 5   | 14.50         | -3.402 | .001 |
|   | Positive Ranks   | 23  | 14.50         |        |      |
|   | Ties             | 104 |               |        |      |
|   | Total            | 132 |               |        |      |
| Knowledge level about IT crimes (Q14)                                   | Negative Ranks   | 8   | 36.25         | -6.367 | .000 |
|   | Positive Ranks   | 68  | 38.76         |        |      |
|   | Ties             | 56c |               |        |      |
|   | Total            | 132 |               |        |      |
| Knowledge level on how to deal with IT crimes (Q15)                     | Negative Ranks   | 8   | 22.50         | -7.261 | .000 |
|   | Positive Ranks   | 75  | 44.08         |        |      |
|   | Ties             | 49  |               |        |      |
|   | Total            | 132 |               |        |      |
| Knowledge level on harms of unlicensed software (Q16)                   | Negative Ranks   | 14  | 34.93         | -5.794 | .000 |
|   | Positive Ranks   | 69  | 43.43         |        |      |
|   | Ties             | 49  |               |        |      |
|   | Total            | 132 |               |        |      |

|  |                |     |       |        |      |
|--|----------------|-----|-------|--------|------|
| Knowledge level on criminal liability of using unlicensed software (Q17) | Negative Ranks | 20  | 35.18 | -6.658 | .000 |
|  | Positive Ranks | 83  | 56.05 |        |      |
|  | Ties           | 29  |       |        |      |
|  | Total          | 132 |       |        |      |
| Knowledge level on adding password to the screen saver of used OS (Q25)  | Negative Ranks | 4   | 21.50 | -7.831 | .000 |
|  | Positive Ranks | 82  | 44.57 |        |      |
|  | Ties           | 43  |       |        |      |
|  | Total          | 129 |       |        |      |
| Knowledge level on creating user accounts (Q26)                          | Negative Ranks | 30  | 38.80 | -2.717 | .007 |
|  | Positive Ranks | 53  | 43.81 |        |      |
|  | Ties           | 47  |       |        |      |
|  | Total          | 130 |       |        |      |
| Knowledge level on creating user accounts (Q27)                          | Negative Ranks | 25  | 34.88 | -5.045 | .000 |
|  | Positive Ranks | 67  | 50.84 | -3.362 | .001 |
|  | Ties           | 38  |       |        |      |
|  | Total          | 130 |       |        |      |
| Knowledge level on creating user accounts (Q28)                          | Negative Ranks | 27  | 35.94 | -3.362 | .001 |
|  | Positive Ranks | 54  | 43.53 |        |      |
|  | Ties           | 49  |       |        |      |
|  | Total          | 130 |       |        |      |
| Knowledge level on Windows firewall (Q29)                                | Negative Ranks | 3   | 48.50 | -7.243 | .000 |
|  | Positive Ranks | 78  | 40.71 |        |      |
|  | Ties           | 39  |       |        |      |
|  | Total          | 120 |       |        |      |
| Knowledge level on Windows defender (Q30)                                | Negative Ranks | 3   | 17.00 | -7.782 | .000 |
|  | Positive Ranks | 80  | 42.94 |        |      |
|  | Ties           | 37  |       |        |      |



|  |                |     |       |        |      |
|--|----------------|-----|-------|--------|------|
|  | Total          | 120 |       |        |      |
| Knowledge level on settings menu of the Android OS (Q36)                   | Negative Ranks | 1   | 14.00 | -5.850 | .000 |
|  | Positive Ranks | 44  | 23.20 |        |      |
|  | Ties           | 40  |       |        |      |
|  | Total          | 85  |       |        |      |
| Knowledge level on screen lock of the Android OS (Q37)                     | Negative Ranks | 12  | 20.13 | -3.037 | .002 |
|  | Positive Ranks | 32  | 23.39 |        |      |
|  | Ties           | 41  |       |        |      |
|  | Total          | 85  |       |        |      |
| Knowledge level on adding owner information to the Android OS (Q38)        | Negative Ranks | 22  | 39.09 | -.194  | .868 |
|  | Positive Ranks | 37  | 24.59 |        |      |
|  | Ties           | 26  |       |        |      |
|  | Total          | 85  |       |        |      |
| Knowledge level on opening e-mails from strangers (Q39)                    | Negative Ranks | 5   | 26.60 | -6.930 | .000 |
|  | Positive Ranks | 70  | 38.81 |        |      |
|  | Ties           | 48  |       |        |      |
|  | Total          | 123 |       |        |      |
| Knowledge level on opening attachments in the e-mails from strangers (Q40) | Negative Ranks | 10  | 21.80 | -4.640 | .000 |
|  | Positive Ranks | 44  | 28.80 |        |      |
|  | Ties           | 69  |       |        |      |
|  | Total          | 123 |       |        |      |
| Knowledge level on opening attachments of the e-mails from strangers (Q41) | Negative Ranks | 23  | 37.30 | -.846  | .398 |
|  | Positive Ranks | 39  | 28.08 |        |      |
|  | Ties           | 61  |       |        |      |
|  | Total          | 123 |       |        |      |
| Knowledge level on filtering settings of e-mails (Q42)                     | Negative Ranks | 11  | 31.68 | -6.687 | .000 |
|  | Positive Ranks | 75  | 45.23 |        |      |
|  | Ties           | 37  |       |        |      |
|  | Total          | 123 |       |        |      |

|  |                |     |       |        |      |
|--|----------------|-----|-------|--------|------|
| Knowledge level on security settings of web browsers (Q43)               | Negative Ranks | 18  | 28.89 | -5.081 | .000 |
|  | Positive Ranks | 59  | 42.08 |        |      |
|  | Ties           | 48  |       |        |      |
|  | Total          | 125 |       |        |      |
| Knowledge level on harms of sharing personal information via SNSs (Q44)  | Negative Ranks | 19  | 26.79 | -4.502 | .000 |
|  | Positive Ranks | 52  | 39.37 |        |      |
|  | Ties           | 54  |       |        |      |
|  | Total          | 125 |       |        |      |
| Knowledge and skill level on security and privacy settings of SNSs (Q45) | Negative Ranks | 15  | 36.90 | -5.411 | .398 |
|  | Positive Ranks | 67  | 42.53 |        |      |
|  | Ties           | 43  |       |        |      |
|  | Total          | 125 |       |        |      |

---