FROM GENERAL TECHNOLOGY FAMILIARITY TO ANTI-SPYWARE PROGRAM ADOPTION: COMPARISON BETWEEN THE U.S. AND SOUTH KOREA

A Thesis

Presented to

the Faculty of the College of Business

Morehead State University

In Partial Fulfillment

of the Requirements for the Degree

Master of Science

by

Dong-Heon Kwak

April 7, 2009

Accepted by the faculty of the College of Business, Morehead State University, in partial fulfillment of the requirements for the Master of Science degree.

Donna L. Kizzier
Director of Thesis

Master's Committee: Donna Kizzier, Chair

April 7, 2009
Date

FROM GENERAL TECHNOLOGY FAMILIARITY TO ANTI-SPYWARE PROGRAM ADOPTION: COMPARISON BETWEEN THE U.S. AND SOUTH KOREA

Dong-Heon Kwak, M.S.
Morehead State University, 2009

Director of Thesis:

Spyware is a big threat, posing severe privacy and security issues. The best way to eliminate spyware, and thus reduce the threat, is to adopt anti-spyware programs. While previous studies identified various determinants of anti-spyware adoption, some factors have not been examined. Based on the theory of reasoned action, the theory of planned behavior, and the technology acceptance model, this study attempted to indentify why users adopt anti-spyware programs and examined causal relationships between the following variables: general technology familiarity, knowledge of spyware, perceived risk of spyware, and trust of anti-spyware programs. This study also divided general technology familiarity into computer, Internet, and security familiarity. Lastly, differences between U.S. and South Korea were identified. Based on research objectives, this study proposed 11 hypotheses and empirically tested them by using confirmatory factor analysis (CFA), structural equation modeling (SEM), and analysis of covariance (ANCOVA). After hypotheses testing, this study found that general technology familiarity does not significantly influence intention of adoption. However, computer and security familiarity were important predictors of knowledge of spyware; and Internet familiarity was a determinant of perceived risk and trust in the U.S. and South Korea. Significant differences were found between the U.S. and South Korea with regard to how computer familiarity, familiarity, security familiarity, knowledge of spyware, perceived risk of spyware, trust of anti-spyware programs, and intention to adopt anti-spyware programs are perceived.

Accepted by: , Chair

Table of Contents

Abstract ---------- i

List of Tables ---------- vi

List of Figures ---------- viii

Chapter 1: Introduction ---------- 1

1. Statement of Problem ---------- 1
2. Purpose of the Study ---------- 3
3. Definition of Spyware ---------- 4
4. Significance of the Study ---------- 5
5. Delimitations of the Study ---------- 6
6. Organization of the Thesis ---------- 7

Chapter 2: Literature Review ---------- 8

1. Theoretical Background of Protective Technology Acceptance --- 8
   (1) Theory of Reasoned Action and Planned Behavior Theory - 8
   (2) Technology Acceptance Model ---------- 10
2. Empirical Findings of Previous Studies ---------- 11
3. Motivation for Comparison between the U.S. and South Korea --- 16
4. Descriptions of Theoretical Variables ---------- 19
   (1) Adoption Intention ---------- 19
   (2) General Technology Familiarity ---------- 19
      a. Computer Familiarity ---------- 21
      b. Internet Familiarity ---------- 23
      c. Security Familiarity ---------- 24
   (3) Knowledge of Spyware ---------- 25
   (4) Perceived Risk of Spyware ---------- 26
   (5) Trust of Anti-Spyware Programs ---------- 27
5. Research Model and Hypotheses Development ---------- 29
   (1) General Technology Familiarity ---------- 32
   (2) Knowledge of Spyware ---------- 33
   (3) Perceived Risk of Spyware ---------- 34

(4) Trust of Anti-Spyware Programs ---------------------------- 36
(5) Differences Between the U.S. and South Korea ------------ 36

Chapter 3: Research Methodology --- 40
1. Outline of the Research Methodology ----------------------------- 40
2. Population and Sample -- 42
3. Survey Instrument Development -------------------------------------- 42
(1) General Technology Familiarity ---------------------------- 43
(2) Knowledge of Spyware -------------------------------------- 45
(3) Perceived Risk of Spyware --------------------------------- 46
(4) Trust of Anti-Spyware Programs --------------------------- 47
(5) Intention to Adopt Anti-Spyware Programs --------------- 47
4. Pilot Test --- 48
5. Procedure for Main Study --- 49
6. Data Analysis -- 50
7. Statistics for Main Study -- 50
(1) Analysis of Covariance ------------------------------------- 50
(2) Exploratory Factor Analysis ------------------------------- 51
(3) Confirmatory Factor Analysis ------------------------------ 51
(4) Structural Equation Modeling ------------------------------ 53

Chapter 4: Results --- 56
1. Data Screening -- 56
2. Demographic Information -- 56
3. Measurement Model --- 59
(1) Descriptive Statistics and ANCOVA ------------------- 59
(2) Reliability Test --- 60
(3) Exploratory Factor Analysis --------------------------- 61
(4) Confirmatory Factor Analysis ------------------------- 61
(5) Measurement Model Fit -------------------------------- 63
(6) Unidimensionality and Convergent Validity --------- 64
a. Computer Familiarity --------------------------------- 65
b. Internet Familiarity ---------------------------------- 66

c. Security Familiarity ---------------------------- 67

d. Knowledge of Spyware -------------------------- 68

e. Perceived Risk of Spyware ------------------------ 69

f. Trust of Anti-Spyware Programs ----------------- 70

g. Intention to Adopt Anti-Spyware Programs ------- 71

(7) Internal Consistency ---------------------------------- 72

(8) Discriminant Validity --------------------------------- 73

4. Structural Model --- 74

(1) Initial Model -- 74

(2) Revised Model --- 77

(3) Model Fit of Structural Model ---------------------- 80

Chapter 5: Discussion and Conclusion ------------------------------------ 83

1. Discussion of Results -- 83

2. Implications --- 89

3. Limitations -- 90

4. Future Research --- 91

5. Conclusion --- 92

References --- 93

Appendix A: Descriptive Statistics and ANCOVA for Individual Items ----------- 102

Appendix B: Results of Exploratory Factor Analysis ------------------------- 104

Appendix C: Survey Instrument (English) ------------------------------------ 106

Appendix D: Survey Instrument (Korean) ------------------------------------ 111

IRB Approval

List of Tables

Table 1-1. Classification of Spyware -- 5

Table 2-1. Demographic, Economic and Internet-Related Profile of the U.S. and South Korea -- 17

Table 2-2. Summary of Research Hypotheses ------------------------------------ 39

Table 3-1. Source and Results of Exploratory Factor Analysis and Confirmatory Factor Analysis for Computer Familiarity Items ------- 44

Table 3-2. Source and Results of Exploratory Factor Analysis and Confirmatory Factor Analysis for Internet Familiarity Items --------- 45

Table 3-3. Source and Results of Exploratory Factor Analysis and Confirmatory Factor Analysis for Security Familiarity Items -------- 45

Table 3-4. Source and Results of Exploratory Factor Analysis and Confirmatory Factor Analysis for Knowledge of Spyware Items ---- 46

Table 3-5. Source and Results of Exploratory Factor Analysis and Confirmatory Factor Analysis for Perceived Risk of Spyware Items 46

Table 3-6. Source and Results of Exploratory Factor Analysis and Confirmatory Factor Analysis for Trust of Anti-Spyware Programs Items -- 47

Table 3-7. Source and Results of Exploratory Factor Analysis and Confirmatory Factor Analysis for Intention to Adopt Anti-Spyware Programs Items --- 48

Table 3-8. Summary of Statistics for Hypotheses --------------------------------- 55

Table 4-1. Demographic Profile of the Survey Respondents --------------------- 57

Table 4-2. Anti-Spyware Program, Computer, and Internet Usage -------------- 58

Table 4-3. Reliability Test --- 60

Table 4-4. Fit Indices Used in this Study -- 62

Table 4-5. Goodness of Fit Indices for the Measurement Model ----------------- 64

Table 4-6. Factor Loading and Squared Multiple Correlation of Computer Familiarity --- 65

Table 4-7. Scale Refinement of Computer Familiarity --------------------------- 65

Table 4-8. Factor Loading and Squared Multiple Correlation of Internet Familiarity --- 66

Table 4-9. Scale Refinement of Internet Familiarity ----------------------------- 66

Table 4-10. Factor Loading and Squared Multiple Correlation of Security Familiarity ---------- 67

Table 4-11. Scale Refinement of Security Familiarity ---------- 67

Table 4-12. Factor Loading and Squared Multiple Correlation of Knowledge of Spyware ---------- 68

Table 4-13. Scale Refinement of Knowledge of Spyware ---------- 68

Table 4-14. Factor Loading and Squared Multiple Correlation of Perceived Risk of Spyware ---------- 69

Table 4-15. Scale Refinement of Perceived Risk of Spyware ---------- 69

Table 4-16. Factor Loading and Squared Multiple Correlation of Trust of Anti-Spyware Programs ---------- 70

Table 4-17. Scale Refinement of Trust of Anti-Spyware Programs ---------- 70

Table 4-18. Factor Loading and Squared Multiple Correlation of Intention to Adopt Anti-Spyware Programs ---------- 71

Table 4-19. Scale Refinement of Intention to Adopt Anti-Spyware Programs ---- 71

Table 4-20. Reliability and Variance Extracted ---------- 72

Table 4-21. Correlation and Discriminant Validity in the U.S. ---------- 73

Table 4-22. Correlation and Discriminant Validity in the South Korea ---------- 73

Table 4-23. Standardized Path Coefficients and Significances of Initial Model -- 76

Table 4-24. Standardized Path Coefficients and Significances of Revised Model 79

Table 4-25. Goodness of Fit Indices for the Anti-Spyware Adoption Model ----- 80

Table 4-26. Results of Hypothesis Testing of Initial Model ---------- 81

Table 4-27. Results of Hypothesis Testing of Revised Model ---------- 82

List of Figures

Figure 2-1. Empirical Findings of Agarwal and Karahanna ------------------------ 12

Figure 2-2. Empirical Findings of Strite and Karahanna --------------------------- 12

Figure 2-3. Empirical Findings of Intention to Adopt Anti-Spyware Programs - 13

Figure 2-4. Empirical Findings of Anti-Spyware Program Adoption ------------ 14

Figure 2-5. Empirical Findings of Online Shopping ------------------------------ 15

Figure 2-6. Empirical Findings of Online Consumer Purchasing ---------------- 15

Figure 2-7. Dimensions of General Technology Familiarity ---------------------- 21

Figure 2-8. Dimensions of Trust -- 29

Figure 2-9. Belief → Intention Framework -- 30

Figure 2-10. Belief → Attitude → Intention Framework ---------------------------- 31

Figure 2-11. Proposed Research Model of Current Study ------------------------- 31

Figure 3-1. Research Methodology --- 41

Figure 3-2. Measurement Model --- 52

Figure 3-3. Structural Equation Model --- 54

Figure 4-1. Initial Structural Model -- 74

Figure 4-2. Revised Structural Model -- 77

Chapter 1

Introduction

Malware is software designed to infiltrate or damage a computer system without the user's consent. It includes viruses, spyware, and spam. This study examines an anti-spyware program adoption model that extends previous studies of technology acceptance. This first chapter addresses the statement of problem, purpose of the study, definition of spyware, significance of the study, delimitation of the study, and organization of the thesis.

1. Statement of Problem

With the development of computer technology and the Internet, the population of internet users, including online shoppers, has radically increased, enabling companies (e.g. Amazon.com and e-bay) to obtain customer information efficiently. However, some complicated data collection by spyware has raised serious privacy and security concerns of users, companies, and developers (Zhang, 2005). These issues emerged because spyware is secretly downloaded on a user's computer to control and monitor the user's behaviors. Although the original intent of spyware was to create software that would remain hidden from users until the users need to be rescued from a programming or application snag, at which time the software would pop up and help them solve their computer problems, it has become a type of malware (Baker, 2006).

Spyware poses severe privacy and security issues to users of electronic commerce (e-commerce) and mobile commerce (m-commerce) (Shukla & Nah,

2005) by limiting their online activities. According to John Edwards (2001), spyware is just one of many startling examples of how people's privacy is being eroded. That is, obtaining private information without consent by using spyware is to infringe upon the users and to violate users' privacy. Also, few people or corporations believe spyware is beneficial to the computing experience, but this issue has not been well studied (Stafford & Urbaczewski, 2004). Fortunately, researchers and business practitioners have recently begun to pay attention to negative technology such as spyware (Dinev & Hu, 2007).

According to the *Economist* (2004), the top three spyware firms in the U.S claim their software is installed on approximately 100 million PCs. Microsoft claims that half of all computer crashes reported by its customers were caused by spyware and its equivalents (Spring, 2004). Dell pronounced that spyware is responsible for about 12% of all technical support calls and accounts for the biggest category of customer complaints (Asaravala, 2004).

While normal computer users generally recognize that direct attacks by viruses or hackers are major threats to them, they tend not to regard spyware as an important issue because the threat by spyware is an indirect infiltration in the form of monitoring programs surreptitiously installed on computers (Gibson, 2005). The best way to prevent infiltration from spyware is to adopt anti-spyware programs. Anti-spyware programs are the most widely recommended solution; the programs implement features that prevent, detect, and remedy the problems caused by spyware (Lee & Kozar, 2008).

According to Beith (2005), more than 100 million Internet users downloaded

Lavasoft's free anti-spyware programs. Some big companies such as Microsoft have also provided anti-spyware programs. Studies have identified that more than 80% of current spyware problems could be identified and resolved by using anti-spyware programs, and thus, security specialists strongly encourage Internet users to use anti-spyware programs (Lee & Kozar, 2008). According to *Consumer Reports* (2008), 33% of Internet users in their survey did not use software to block or remove spyware in 2007. In sum, anti-spyware programs can effectively protect users from spyware, and their low adoption rate creates problems for users in the Internet world.

2. Purpose of the Study

The purpose of this study is to identify factors of intention to adopt anti-spyware programs and to examine how individuals' technology familiarity influences intention to adopt anti-spyware programs. This study identifies three dimensions of technology familiarity: computer familiarity, Internet familiarity, and security familiarity. Also, other factors of anti-spyware program adoption such as knowledge, perceived risk, and trust are examined, and their relationships are investigated. Lastly, this study examines whether the research model adopted in U.S. fits in South Korea. If any differences are identified between the cultures, the reasons for these differences are examined.

3. Definition of Spyware

To examine anti-spyware program adoption, this study employs two terms of Dinev and Hu (2007)[1]: negative technologies and protective technologies. Negative technologies are defined as "those that are designed to disrupt or harm their users, such as computer viruses, spyware, and tools for breaking into systems and databases" (p387). On the other hand, protective technologies refers to "those that are designed to deter, neutralize, disable, or eliminate the negative technologies or their effectiveness, such as anti-virus software, anti-spyware tools, firewalls, and intrusion detection technologies" (p387).

Spyware is generally defined as programs that act as data sensors and illicitly collect and transmit information about end users, and then send it back to a third party (Cohen, 2003; Kenyon, 2004). Spyware is the name given to the class of software that is surreptitiously installed on a user's computer and monitors a user's activity and reports back to a third party on that behavior (Daniels, 2004). As, a general class of remote monitoring applications, spyware has created problems so severe that network administrators consider it a greater threat than unsolicited email (Stafford & Urbaczewski, 2004). Also, spyware asserts control over a user's computer without his/her consent (Stafford & Urbaczewski, 2004). One of the protective technologies, anti-spyware programs are defined as the programs designed to detect, block, and remove spyware. Table 1-1 displays Lee

[1] Besides these two terms, the authors also present positive technologies, which refer to "those technologies that are designed to benefit their users in terms of productivity, efficiency, competitiveness, or entertainment" (p387). Positive technologies include office programs, ERP systems, e-commerce technologies, and others.

and Kozar's (2005) classification of spyware and their definitions.

Table 1-1. Classification of Spyware

Class	Definition
Adware	Programs that monitor Internet users' online activities to initiate pop-up advertising or other targeted marketing purposes.
Keyloggers	Programs that capture and record internet users' every keystroke, including personal information and passwords.
Trojans	Malicious programs that appear as harmless or desirable applications, but are designed to cause loss or theft of computer data, or even to destroy the system.
Scumware	Programs that alter the content of Web sites internet users are accessing, changing the normal links to reroute them to other Web sites.
Dialers	Programs typically used by vendors serving pornography via the internet.
Browser Hijackers	Programs that run automatically every time Internet users start their Internet browser to gather information on the user's surfing habits.

Lee & Kozar (2005) (p.74)

4. Significance of the Study

This study will make a contribution to many groups including researchers, practitioners, and educators. While studies exist related to anti-spyware adoption models, most empirical studies are restricted to the U.S. Comparison between the U.S. and South Korea will provide additional international insight for the field. This study will also test and extend the existing model of anti-spyware program adoption.

From a practitioner's perspective, this study will aid in the management of organizational Web sites by helping firms provide the Internet user with knowledge on negative programs, such as spyware and viruses. This will reduce Internet users' concern and increase visitation rates. Also, an understanding of adoption factors by anti-spyware sites can help improve uptake.

Contributions to educators are also expected. First, college instructors will be able to use the results to design relevant security courses. Second, every computer user is a potential victim of spyware. Suitable education about negative and protective technologies will reduce potential risks.

5. Delimitations of the Study

As with most research, this study has delimitations. First, this study considers acceptance of protective information technology by end users. Nowadays, protective information technology includes various programs, such as anti-spyware, anti-virus, and others. However, this study is restricted to anti-spyware program adoption.

Second, while spyware problems are considered in the organizational and interorganizational perspective as well as the individual perspective, the anti-spyware program adoption of this study is limited to the individual perspective.

The third delimitation is of selecting undergraduate and graduate college students in the U.S. and South Korea as respondents. Although this choice could be considered a delimitation, the use of college students as a sample for technology acceptance research is common and considered acceptable when the students intend to use the technology. Also younger people are regarded as having more Internet savvy than standard computer users.

This study also uses a convenience sample of students from only one university in the U.S. and one university in South Korea. The principle of probability sampling indicates that a sample represents the population if all members of the population have an equal chance of being selected in the sample (Babbie, 1995). The convenience sample being used lacks some representativeness of the wider protective technology user population. Sampling bias from using one university in each country studied could exist.

6. Organization of the Thesis

Chapter 1 presents the scope of the study and discusses contributions, limitations and the organization of the study. Chapter 2 provides the reader with a relevant review of the literature on the technology acceptance model, and a review of technology familiarity, as well as other variables that influence protective information technology. The conceptual research model is also presented based on constructs derived from the literature review along with hypotheses that will be tested. Chapter 3 presents the research methodology for the study. Chapter 4 will summarize the results of the study while Chapter 5 will provide conclusions and suggestions for further research.

Chapter 2

Literature Review

This chapter begins by reviewing three theoretical models related to protective technology adoption: the theory of reasoned action, the theory of planned behavior, and the technology acceptance model. Next, previous empirical studies of anti-spyware adoption are reviewed and variables of the study are discussed. The final section of the chapter introduces the research model and hypotheses.

1. Theoretical Background of Protective Technology Acceptance

In this study, the anti-spyware program adoption model is based on three theories: the theory of reasoned action, the planned behavior theory, and the technology acceptance model. This section discusses each of these three theories. Based on the theories, five constructs (i.e. technology familiarity, knowledge of spyware, perceived risk of spyware, trust of anti-spyware program, and intention to adopt anti-spyware program) are derived and discussed.

(1) Theory of Reasoned Action and Planned Behavior Theory

According to the theory of reasoned action (TRA) (Fishbein & Ajzen 1975, p.16), an individual's behavior is predicted by his or her intention to perform the behavior. The intention is influenced by two factors: (1) attitude toward the behavior, a function of beliefs about consequences of the behavior, and (2) subjective norms concerning the behavior, a function of normative beliefs about the behavior. Attitude toward the behavior is an individual's positive or negative feelings about performing the behavior. A subjective norm is an individual's perception of how most people who are important to him or her think about whether he or she should or should not perform the behavior.

Extended from TRA, the planned behavior theory (PBT) is about the relationship between attitude and behavior. PBT has been applied to studies of the relations among beliefs, attitudes, behavioral intentions and behaviors in information systems research, especially computer-related human behaviors. PBT is used in information systems research because it can successfully capture individual, social, and situational factors impacting an individual's decision related to the use of information systems (Ajzen, 1988).

Because PBT has been an effective theory in explaining and predicting the adoption of new information technologies, it is a good base for examining the adoption of anti-spyware programs. In PBT, key factors in behavioral intention are: attitude toward the act, subjective norm, and perceived behavioral control (Ajzen, 1988). TRA and PBT both maintain that attitude completely mediates the relationship between *beliefs* and *intention.*

This study adopts the *beliefs* → *attitudes* → *intention* framework of TRA and PBT to the spyware adoption context and incorporates other variables pertinent to research questions related to intention to adopt anti-spyware program.

(2) Technology Acceptance Model

While some of the research on technology adoption has examined the organizational level (Bassellier, Benbasat, & Reich, 2003) and the interorganizational level (Hart & Saunders, 1997), a number of information systems studies have focused on how and why individuals adopt new technologies (Venkatesh, Morris, Davis, & Davis, 2003). The current study also focuses on the individual level of technology adoption by using intention as a dependent variable (e.g. Davis, 1989).

In response to the limitations related to TRA in predicting and explaining user adoption of a new technology, Davis (1989) and Davis, Bagozzi, and Warshaw (1989) developed the technology acceptance model (TAM) as an extension of TRA. Similar to TRA and PBT, the original TAM indicated that attitudes toward a new technology influence its adoption and use. TAM also attempted to explain the voluntary acceptance of a new technology as influenced by two beliefs: (1) the perceived usefulness, and (2) the perceived ease of use. The original TAM (Davis et al. 1989) empirically tested a partial mediation of attitude, while subsequent studies eliminated attitude as a predictor of technology acceptance (Venkatesh & Davis, 1996, 2000). Accordingly, the majority of TAM models suggest a direct path from perceived usefulness and perceived ease of use to behavioral intention, which contradicts TRA and PBT. Moreover, the Unified Theory of Acceptance and Use of Technology (UTAUT) model (Venkatesh et al. 2003) eliminated attitude by indicating that attitude will not have a direct effect on intention when performance and effort expectancy constructs are included in the model. UTAUT considers "any observed relationship between attitude and intention to be spurious and resulting from omission of the other key predictors" (p.455).

This study employs the ***beliefs* → *intention*** framework of TAM as well as the ***belief* → *attitude* → *intention*** framework of TRA and PBT in explaining and predicting user behavior toward anti-spyware program adoption.

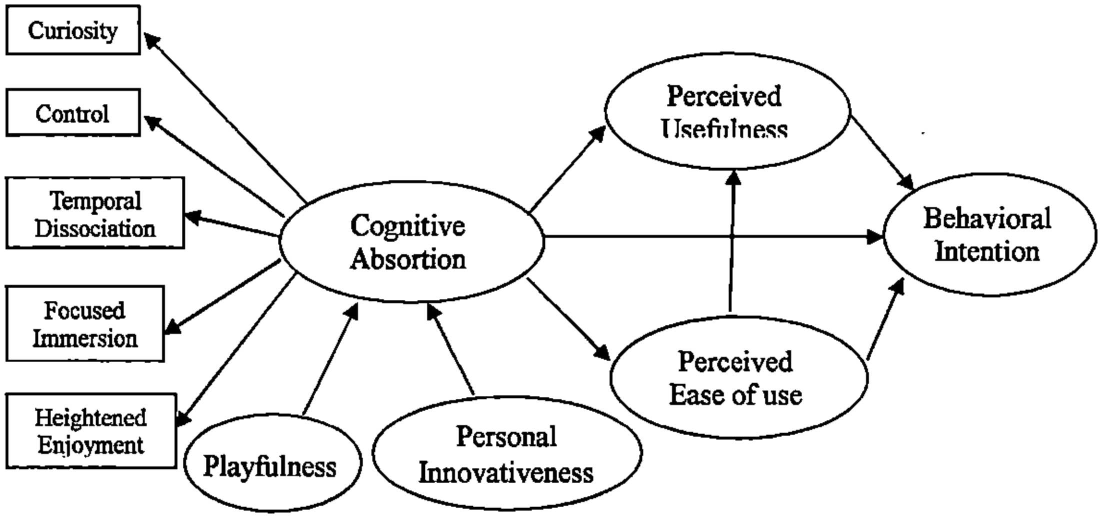
2. Empirical Findings of Previous Studies

Several studies have been conducted to examine the technology acceptance based on TRA, PBT, or TAM. Based on PBT and innovation diffusion theory (IDT), Taylor and Todd (1995) argued that perceived usefulness, ease of use, and compatibility were factors of attitude and found that perceived usefulness had a significant effect on attitude.

Yi, Jackson, Park, and Probst (2006) developed an integrated model by incorporating IDT with the PBT and TAM for predicting personal data assistant (PDA) adoption by healthcare professionals. Karahanna, Straub, and Chervany (1999) incorporated IDT with TRA to address individuals' pre-adoption and post-adoption belief and attitude toward Windows technology.

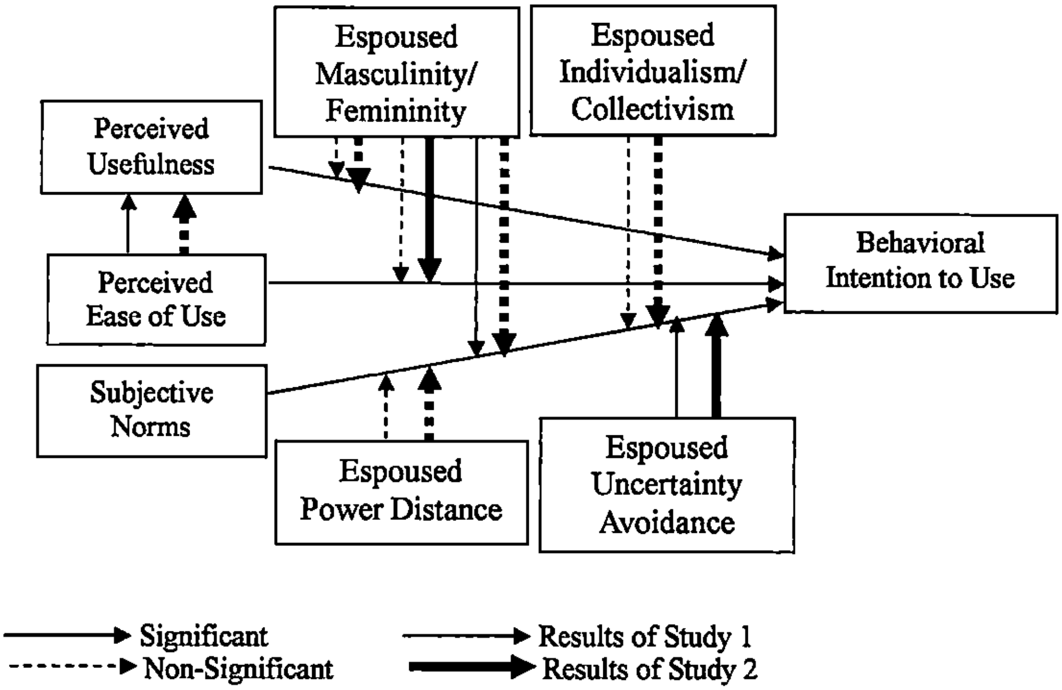
Agarwal and Karahanna (2000) empirically found that users' cognitive absorption is posited to be a proximal antecedent of perceived usefulness and perceived ease of use. Figure 2-1 summarizes Agarwal and Karahanna's findings.

Figure 2-1. Empirical Findings of Agarwal and Karahanna (2000)



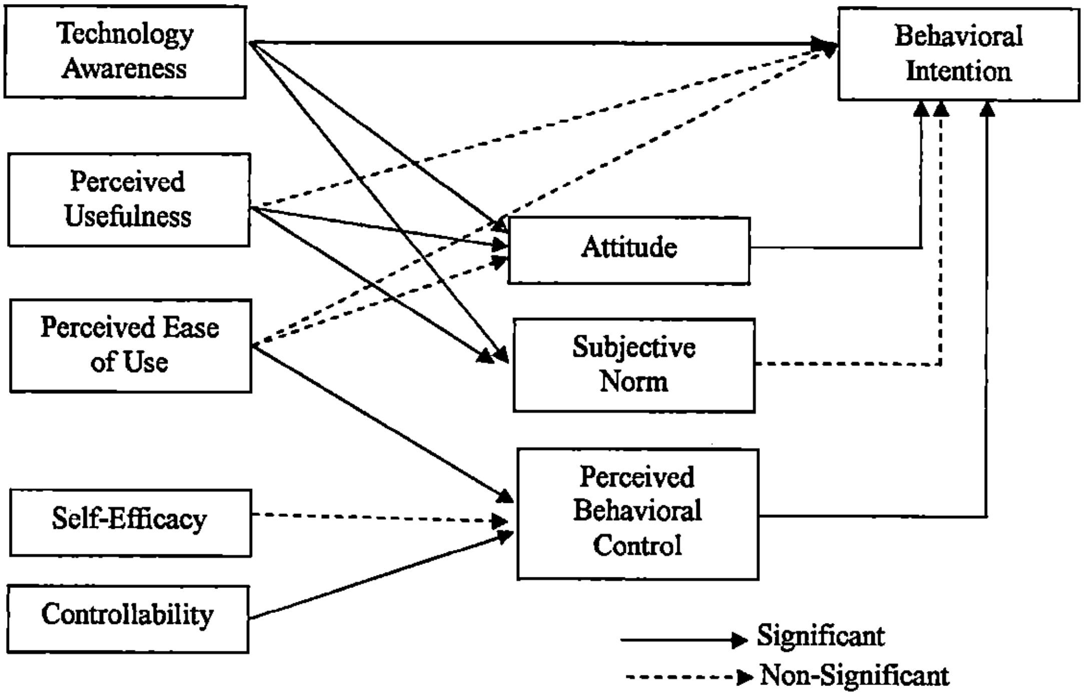
Strite and Karahanna (2006) incorporated national cultural values of masculinity/femininity, individualism/collectivism, power distance, and uncertainty avoidance into an extended model of technology acceptance as moderators. Figure 2-2 illustrates Strite and Karahanna's findings.

Figure 2-2. Empirical Findings of Strite and Karahanna (2006)



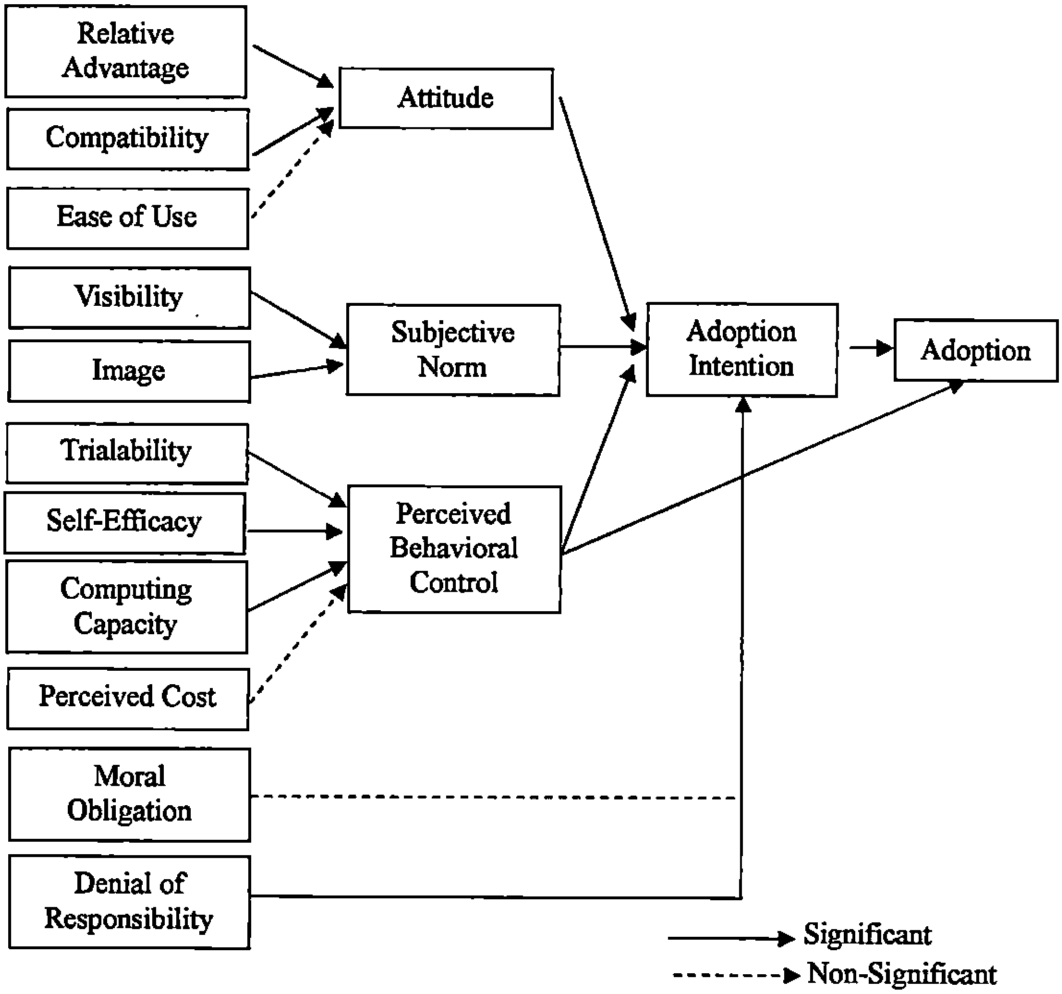
In the context of anti-spyware adoption, combining PBT with TAM, Dinev and Hu (2007) empirically found the factors of intention to adopt anti-spyware programs. In protective technology acceptance, according to Dinev and Hu (2007), awareness of spyware is the key factor of intention to adopt anti-spyware programs. Figure 2-3 summarizes Dinev and Hu's findings.

Figure 2-3. Empirical Findings of Intention to Adopt Anti-Spyware Programs (Dinev & Hu, 2007)



Lee and Kozar (2008) also found determinants of adoption intention for anti-spyware programs. They incorporated PBT, IDT, and information technology ethics and morality and found the determinants of intention to adopt anti-spyware programs. Figure 2-4 summarizes Lee and Kozar's findings.

Figure 2-4. Empirical Findings of Anti-Spyware Adoption (Lee & Kozar, 2008)



In the context of online shopping, several researchers have examined familiarity, trust, and perceived risk as predictors of behavioral intention. Gefen, Karahanna, and Straub (2003) incorporated trust and TAM and found determinants of trust and perceived ease of use. Van Slyke, Shim, Johnson, and Jiang (2006) empirically found the relationship between concern for information privacy and trust and risk perception. Figure 2-5 displays Gefen et al.'s findings and Figure 2-6 illustrates Van Slyke et al.'s findings.

Figure 2-5. Empirical Findings of Online Shopping (Gefen et al. 2003)

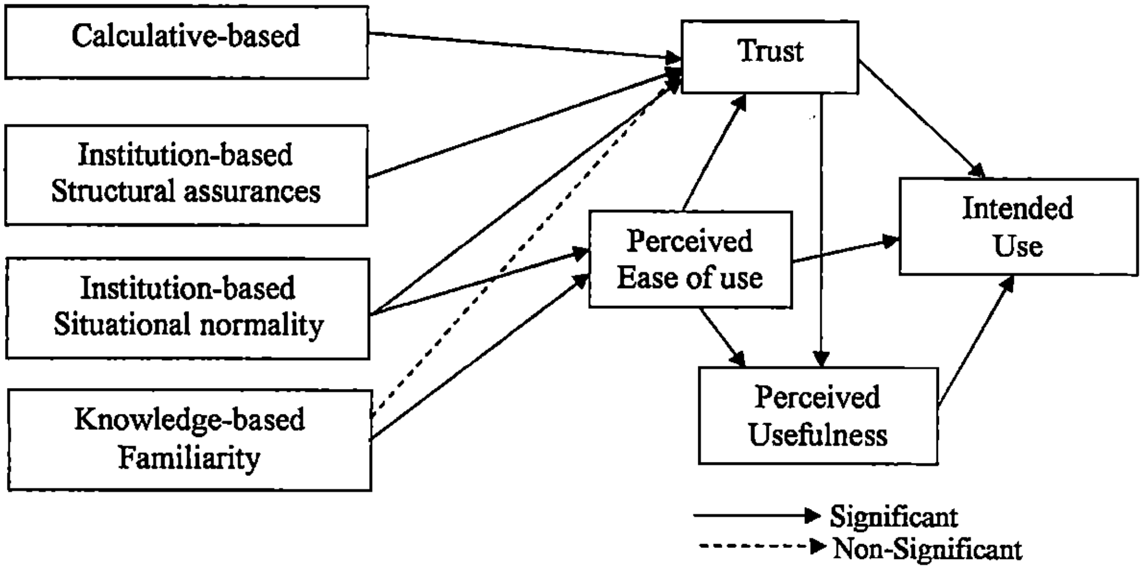
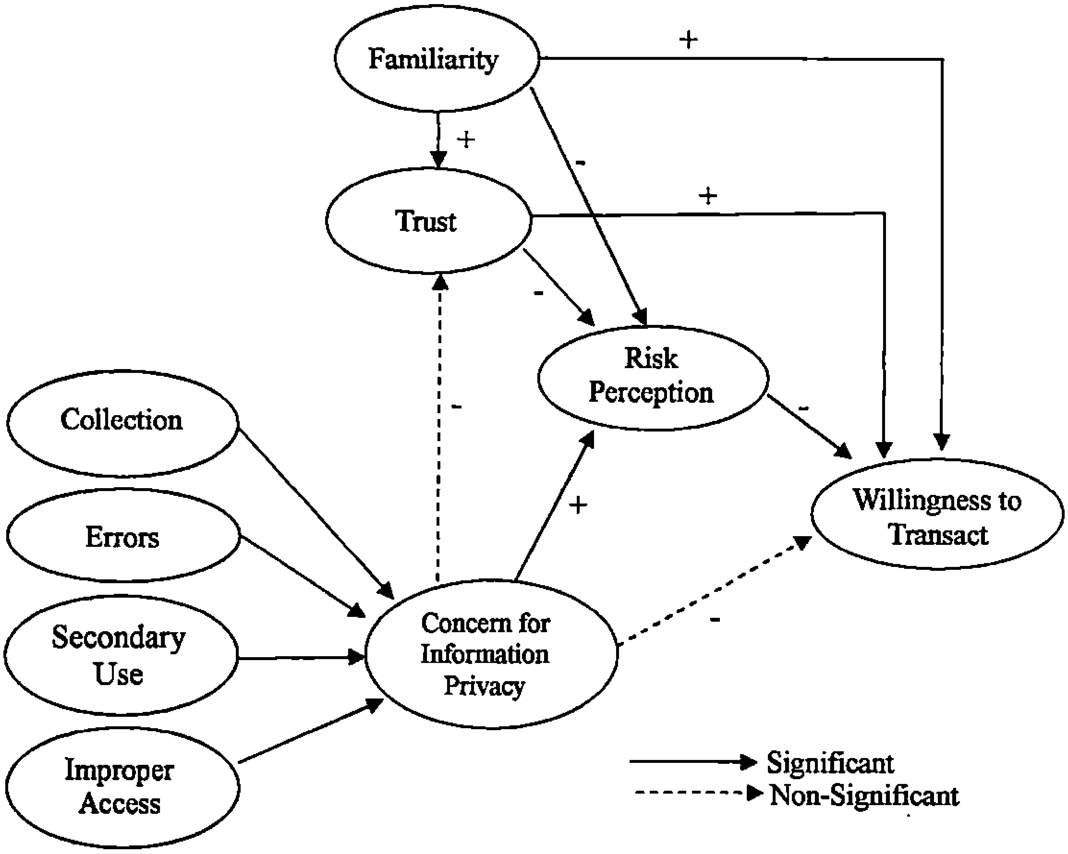

Calculative-based
Institution-based Structural assurances
Institution-based Situational normality
Knowledge-based Familiarity
Trust
Perceived Ease of use
Intended Use
Perceived Usefulness
Significant
Non-Significant

Figure 2-6. Empirical findings of Online Consumer Purchasing

(Van Slyke et al. 2006)



3. Motivation for Comparison between the U.S. and South Korea

Globalization of business has emphasized the need for understanding the management of organizations that span different nations and cultures, and cultural differences between countries can influence the effectiveness and efficiency of information systems deployment (Karahanna, Evaristo, & Srite, 2002). Thus, cross-cultural information systems research is necessary and should be developed further.

The U.S. is the most developed country in IS research and development and South Korea is the most dynamic country in introducing and developing IS. South Korea is ranked first among the 30 member countries of the organization for Economic Cooperation and Development (OECD) in terms of broadband access, and has showed rapid growth of Internet use and e-commerce. The rate of Internet penetration in South Korea (70.7%) is equivalent to that in the U.S. (72.5%). Both countries have a developed Internet infrastructure. Table 2-1 displays the demographic, economic and Internet-related profile of the U.S. and South Korea.

Table 2-1. Demographic, Economic and Internet-Related Profile of the U.S. and South Korea

Categories		U.S.	South Korea
Demography	population[1] (2008 est.)	303,824,646	49,232,844
	Ethnic groups[2]	White 78% Black 12.9% Asian 4.4% Others 4.7%	Homogeneous (Korean)
	Literacy[2] (Age 15+ can read and write)	Male: 97.0% Female: 97% Overall: 97% (1979 est.)	Male: 99.2% Female: 96.6% Overall: 97.9% (2002 est.)
	Religions	Protestant 56% Roman Catholic 28% Jewish 2% Other 4% none 10%[2]	Buddhist 26% Protestant 19% Roman Catholic 7% Others 2% None 46%[3]
Economy	GDP per capita[3] (2007)	$45,259	$20,045
	GNI per capita[3] (2006)	$45,498	$20,045
Internet	Internet Usage Users[1]	220,141,969 (2008)	34,820,000 (2008)
	Internet Penetration [1] (Internet use/ Population)	44.1% (2000) 50.0% (2001) 58.0% (2002) 59.2% (2003) 68.8% (2004) 68.1% (2005) 68.1% (2007) 72.5% (2008)	39.6% (2000) 63.3% (2005) 66.5% (2006) 70.7% (2008)

Sources

1) The Internet World Stats. http://www.internetworldstats.com (10/6/2008)

2) The World Factbook. http://www.odci.gov/cia/publications/factbook (10/6/2008)

3) Korean National Statistics Office. http://www.nso.go.kr (10/6/2008)

IS researchers have measured their research models globally and found differences among countries. Cultural differences among countries are the most widely studied factor in Internet usage. Cultural factors influence how security policies are formulated and implemented and also determine how a society will perceive computer security threats (Schmidt, Johnston, Arnett, Chen, & Li, 2008).

Theories developed in one country have met with limited success when applied to other countries (Hofstede, 1993). Thus, a main question that cross-cultural research in information systems attempts to answer is: "Why are successful IS theories and techniques not found to be uniformly effective across cultural borders?" (Karahanna, Evaristo, & Strite, 2005, p.2).

One of the goals of the comparison between the U.S. and South Korea is to examine if the research model adopted in the U.S. can be successfully applied in other countries (e.g. South Korea). If any differences are identified, this study will investigate the factors which influence the differences.

4. Descriptions of Theoretical Variables

(1) Adoption Intention

Since adoption intention is the most important determinant of technology acceptance behavior, it becomes important to examine the direct and indirect influences of other factors on adoption intention (Taylor & Todd, 1995). Adoption intention refers to an individual's motivation to exert effort to adopt a particular technology (e.g. anti-spyware programs).

This study employs adoption intention rather than actual adoption behavior in examining determinants of anti-spyware program adoption. This is not uncommon. Numerous studies of technology acceptance have measured behavior intentions but not behaviors (Agarwal & Prasad, 1998; Karahanna et al. 1999; Venkatesh, 1999, 2000). Prior research has also confirmed a strong correlation between behavioral intentions and actual behavior (Sheppard et al., 1988; Venkatesh & Davis, 2000). The TRA and PBT described the positive relationship between behavioral intentions and actions. In the context of anti-spyware adoption, Lee and Kozar (2008) empirically found that intention to adopt anti-spyware programs is a predictor of anti-spyware program adoption.

(2) General Technology Familiarity

Familiarity is one's understanding of an entity, often based on previous interactions, experience, and learning of "the what, who, how, and when of what is happening" (Gefen, et al. 2003, p.63).

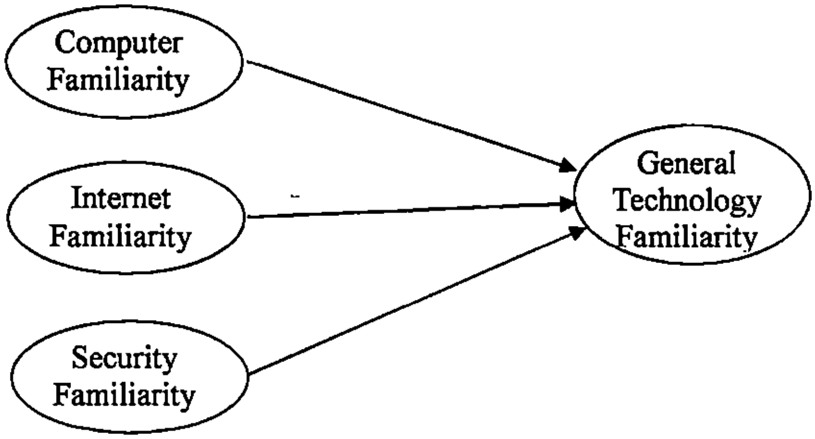
Hoch and Deighton (1989) refer to familiarity as the number of product related experiences accumulated by the consumer. Familiarity appears to serve as an umbrella term and is related to other important constructs including consumer expertise, previous knowledge and belief, and also appears as a necessary condition for the development of expertise and the ability to perform product-related tasks successfully (Ha & Perks, 2005). In turn, familiarity is a main predictor of trust and intention to perform the behavior (Komiak & Benbasat, 2006; Gefen et al, 2003). The familiarity also reduces social uncertainty via increased understanding of what is happening in the present (Luhmann, 1979).

This study defines general technology familiarity as one's understanding based on previous interaction, experience, and learning in terms of computer, Internet, and security.

General technology familiarity is acquired through an individual's prior and direct experiential exchange with technologies related to the computer, Internet, and security. More general technology familiarity implies an increasing amount of accumulated technology knowledge derived from experience from previous successful interaction through the technology (Gefen, 2000).

Based on spyware literature, anti-spyware program adoption is the nexus of interaction for the users among the computer, Internet, and security issues. Spyware causes several problems related to all these elements, including slowing down computer processing and internet speed, violating privacy, and other issues (Freeman & Urbaczewski, 2005; Awad & Fitzgerald, 2005). By examining anti-spyware program adoption, this study divides general technology familiarity into familiarity with the computer, Internet, and security. This study, therefore, tests general technology familiarity in a multidimensional construct (Petter, Straub, & Rai, 2007). Figure 2-7 illustrates the proposed dimensions of this general technology familiarity. The three general technology familiarity dimensions are discussed next.

Figure 2-7. Dimensions of General Technology Familiarity



a. Computer Familiarity

This study defines computer familiarity as a user's understanding of computer technology based on prior interactions, experiences, or knowledge.

Potosky and Bobko (1998) proposed a definition of computer experience based on the understanding of how computers are used. Potosky and Bobko further noted general computer experience as an integral component of general computer ability. They also suggested that the nature and types of experiences with computers are important, not just the frequency of interaction with programming.

Given the growing prevalence and reliance on computer technology, computer familiarity is crucial for succeeding in society (Nelson, Wiese, & Cooper, 1991). For decades, computers have been very important in companies, government, and school, and even at home; thus, computer familiarity has been studied in several aspects. Empirical research has examined why people differ in their levels of computer familiarity.

Dambrot, Watkins-Malek, Silling, Marshall and Garver (1985) investigated the correlations of gender differences in attitudes toward, and involvement with, computers. In addition, Merchant and Sullivan (1983) found that students with lower GPA and math scores generally suffer more from computer phobia. Additionally, Rosen, Sears, and Weil (1987) indicated that women had more negative attitudes regarding computers than men did. They also noted that older students are more computer anxious than younger students, although they do not display more negative attitudes, cognitions, or feelings regarding computer use. Schulenberg, Yutrzenka, & Goham (2006) and Schulenberg and Melton (2008) developed and validated the instruments for computer aversion, computer attitudes, and computer familiarity.

In sum, individuals have different levels of computer familiarity, and thus computer familiarity is a dimension of technology familiarity in anti-spyware program adoption. The following section introduces Internet familiarity as the second dimension of general technology familiarity.

b. Internet Familiarity

The current study defines Internet familiarity as a user's understanding of Internet technology based on prior interactions, experiences, or knowledge. Internet interaction and experience generally include using e-mail, online shopping, reading online articles, searching information, social networking, and online education, and other behaviors involving the Internet.

Early research on the adoption of computers has shown that the extent of a user's experience with certain technology influences his/her attitude and behavior the technology, and more specifically, the perceived usefulness of the technology, and the intention to use it again (Davis, 1989). Since the Internet is a relatively new technology, not all consumers are equally familiar with it; and even when they are, most people use the Internet for information searches rather than for purchasing on-line (Anckar 2003). For example, novices may experience more difficulty in using a site and rate the site's performance poorer than an experienced person.

Preliminary evidence suggests that the higher the level of user's experience with the Internet, the more positive their attitude toward Web sites (Bruner & Kumar, 2000). According to one survey of Internet users, in clarifying the level of experience, 35 % of participants classified themselves as "novices" while 23% classified themselves as "high end novices" (Poston, Stafford, & Hennington, 2005).

In sum, individuals have different levels of Internet familiarity, and thus Internet familiarity is a dimension of technology familiarity in anti-spyware program adoption. As the last dimension of general technology familiarity, this study examines security familiarity.

c. Security Familiarity

Security familiarity is defined as a user's understanding of security issues based on prior interactions, experiences, or knowledge. Security issues include information privacy, computer and Internet security, and others. More than 1.8 million known malware and security risks exist on the Internet, representing an unprecedented threat to online security and privacy (Security, 2008).

Internet users know that spyware is a security problem, so they would like to protect themselves from spyware. In some cases, users are not aggressive in their plans to take protective actions due either to lack of perceived technical skill or lack of recognition of the severity of the computer security (Poston et al. 2005). Security issues such as information privacy have been identified as one of the most important issues of contemporary management practice (Mason, 1986). According to a recent survey of IT executives, security concerns are increasing on the ranking of managements' most important concerns (Luftman & McLean, 2004).

In efforts to reduce the threats posed to information systems security concerns, IT managers devote an increasing amount of resources to threat detection and amelioration (Whitman, 2003). Smith, Milberg, and Burke (1996) developed and validated an instrument that identifies and measures the primary dimensions of individuals' concerns about organizational information privacy practices. The result reflects four dimensions of concern for information privacy: collection, errors, secondary use, and unauthorized access. In the context of spyware, individuals are concerned about secondary use and unauthorized access of information since spyware can trace keystroke and monitor user's Web behavior without consent.

In sum, individuals have different levels of security familiarity, and thus security familiarity is a dimension of general technology familiarity in anti-spyware program adoption.

This section discussed computer familiarity, Internet familiarity, and security familiarity as dimensions of general technology familiarity. In the next section, knowledge of spyware is examined.

(3) Knowledge of Spyware

Knowledge is the body of facts and principles (i.e., information and understanding) accumulated by mankind (i.e., stored in memory) about a domain (Delbridge & Bernard, 1998). Consumer knowledge literature argues that knowledge has a significant and essential influence on the consumer's decision making. In consumer research, knowledge includes two components, product familiarity and expertise (Alba & Hutchison, 1987). In the meantime, consumer knowledge is related to privacy protection, consumer defection, consumer choice, information search, and perceived product category uncertainty (Zhang, 2005). Also, knowledge enables consumers to shorten the time needed to make decisions and reduce the cognitive effort to perform the task (Alba & Hutchinson, 1987).

In this study, knowledge of spyware focuses on general understanding of spyware rather than specific features of spyware. Following the definition of technology awareness (Dinev & Hart, 2006), this study defines knowledge of spyware as a individual's raised consciousness of and interest in knowing about technological issues and strategies to deal with spyware. Zhang (2005) empirically tested four measures to assess the respondents' knowledge of spyware: tracking keystrokes, recording online transactions, monitoring online surfing habits and residing on computers. Zhang (2005) found that the sample in the U.S. was only familiar with the monitoring surfing habits of spyware.

In the following section, perceived risk of spyware as another factor of adoption intention is introduced.

(4) Perceived Risk of Spyware

The concept of perceived risk most often used by consumer researchers defines risk in terms of the consumer's perceptions of the uncertainty and adverse consequences of buying a product or service. This study defines the perceived risk of spyware as an individual's belief regarding the probability of gains or losses associated with spyware (Mayer, Davis, & Schoorman, 1995).

Several studies argued that an individual's perceived risk influences intention to perform the behavior for reducing the risk. LaRose, Rifon, and Enbody (2008) studied the relationship between the level of personal risk and the individual's safety behavior. According to them, moderate amounts of perceived risk increase safe behavior, while low amounts of perceived risk reduce safety because the threat is not considered an important problem. However, intensely perceived risk can also inhibit safe behavior because people suppress their fear rather than cope with the danger.

According to a survey of Poston et al. (2005), the third most highly recognized threat identified by users was spyware, following viruses and spam. Although several major internet risks, caused by spam, spyware, and virus infection, have declined significantly over the past few years, Internet threats are of great concern to Internet users (*Consumer Reports*, 2008). Steve Gibson (2005) indicated spyware as a source of users' concern.

> "Spyware is the PC user's latest and biggest problem; a larger source of worry, concern, and frustration than anything PC users have faced before, and potentially more damaging than the worst computer viruses. Due to the growing use of PCs for personal tax preparation, online banking, investment portfolio management, and real-time e-commerce, the threat from privacy violation and identity theft cannot be ignored (p38)."

Trust of anti-spyware programs, the last factor of study, is examined in the following section.

(5) Trust of Anti-Spyware Programs

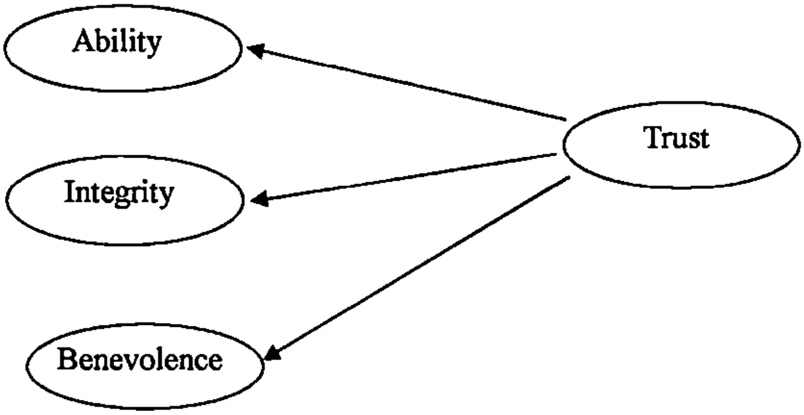
Trust is a widely accepted factor of technology acceptance. Trust plays a central role in helping people overcome perception of risk and insecurity (McKnight, Choudhury, & Kacmar, 2002).

In looking at personalization technology adoption, Komiak and Benbasat (2006) divided trust into cognitive trust and emotional trust; and they found that these two types of trust influence intentions to adopt recommendation agents (e.g. Web-based product-brokering recommendation agents) as a decision aid or as a delegated agent. In the context of e-commerce, Gefen et al. (2003) found a positive relationship between trust and the intention to use a business-to-customers Web site.

Mayer et al. (1995) proposed an integrative definition of trust as "the willingness of a party (trustor) to be vulnerable to the actions of another party (trustee) based on the expectation that the other (trustee) will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party (trustee)" (p712). Meyer et al. (1995) proposed a generic typology of trust, consisting of three dimensions: ability, benevolence, and integrity. These three dimensions are conceptually distinct since they incorporate different elements of cognitive and affective abstraction of trust (Bhattacherjee, 2002).

Building upon the research of Mayer et al.'s work (1995), this study defines trust as the perceived ability, benevolence, and integrity of users in the anti-spyware program adoption. Ability is a characteristic including skill and competence that makes an anti-spyware program have influence within a specific domain (Mayer et al. 1995). Based on this definition, the main ability of an anti-spyware program includes eliminating spyware, and thus protecting users from spyware. Integrity refers to the user's perception that anti-spyware programs are honest (Mayer et al. 1995). Benevolence is the extent to which an anti-spyware program is believed to intend to do good to the user (Mayer et al. 1995). Figure 2-8 models these three dimensions of trust.

Figure 2-8. Dimensions of Trust



Based on Mayer et al. (1995)

5. Research Model and Hypotheses Development

Using the theory of reasoned action as its theoretical background, the research model used for the present study addressed the causal relationships among five variables. The target behavior in this study is anti-spyware program adoption. The research model includes the intention to adopt rather than the behavior of adoption because the role of intention as a strong predictor of behavior has been well established in information systems (Davis 1989; Venkatesh et al. 2003).

Although attitude mediates the impact of beliefs on intention in the theory of reasoned action, attitude is not directly included in the proposed research model because (1) the direct effect of beliefs in information systems contexts is generally stronger than their indirect effect via attitude (Davis et al. 2003) and (2) the influence embodied in attitude is partially captured within the benevolence and integrity dimensions of trust (Bhattacherjee, 2002). Thus, this study conceptualizes technology familiarity, knowledge of spyware, perceived risk of spyware as a *belief*, and trust of anti-spyware program as a *belief* or an *attitude*.

Figure 2-9 illustrates the *belief* → *intention* framework based on TAM and figure 2-10 is the *belief* → *attitude* → *intention* framework based on TRA. Incorporating both the TAM and TRA frameworks, the proposed research model is presented in figure 2-11. In the rest of this section, the relationships in the model, as well as the development of hypotheses, are explained in detail.

Figure 2-9. *Belief* → *Intention* Framework
(Based on Technology Acceptance Model)

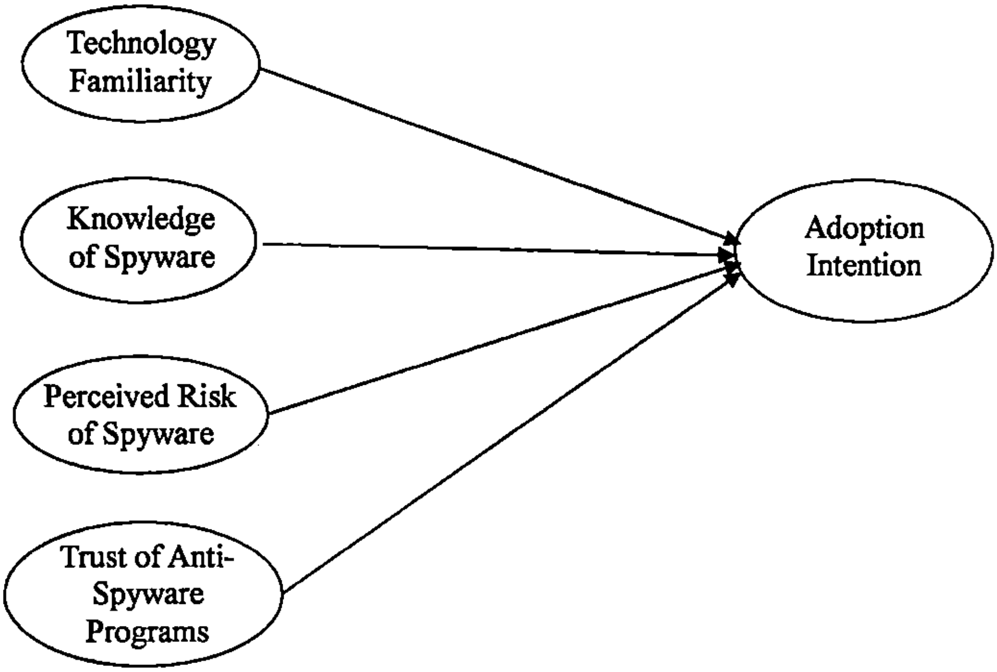


Figure 2-10. *Belief* → *Attitude* → *Intention* Framework
(Based on Theory of Reasoned Action)

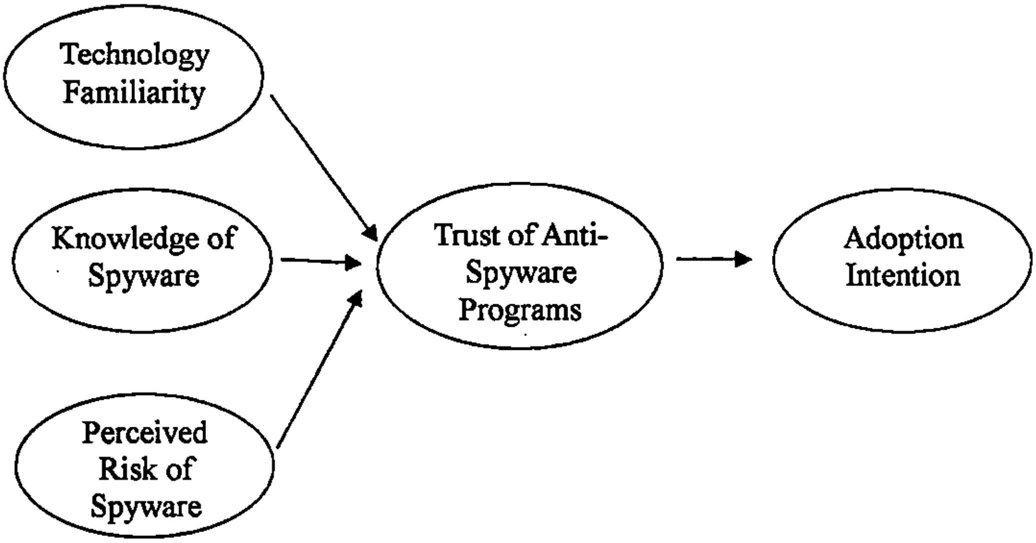
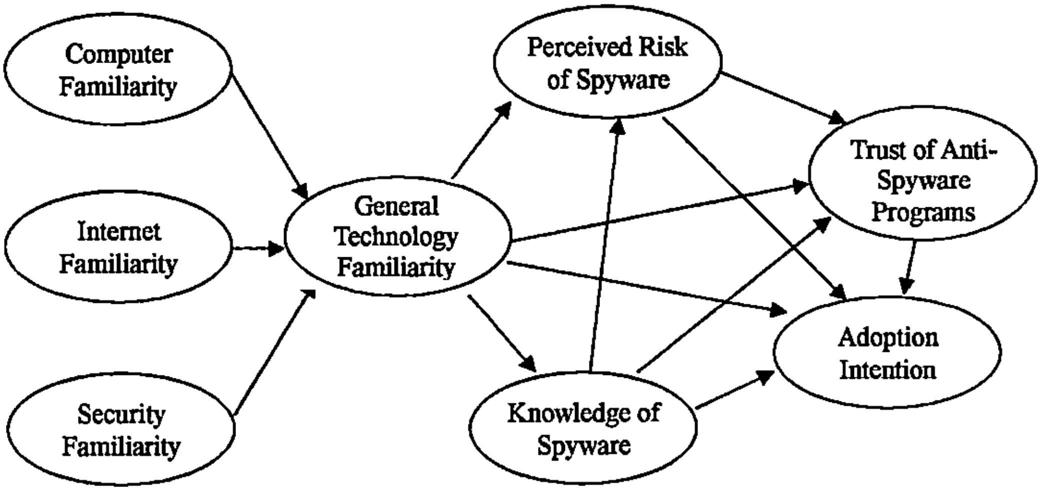


Figure 2-11. Proposed Research Model of Current Study
(The Impact of Knowledge on Anti-Spyware Adoption Model)



(1) General Technology Familiarity

Familiarity is an important predictor of knowledge. In marketing research, familiarity might be generally known information about product categories and brands, based on advertising exposure, product purchase/use, and word-of-mouth effects (Alba & Hutchinson, 1987). Research evidence indicated that brand familiarity reduces the need for information search. For example, Biswas's (1992) study revealed that consumers tend to spend less time shopping for a familiar brand than they do for an unfamiliar brand (Ha & Perks, 2005).

The current study assumes that individuals with familiarity can obtain more specific knowledge. In the same vein, individuals' previous experience and knowledge about technologies affect specific knowledge of spyware. In turn, when individuals have more familiarity with general technology in terms of the computer, internet, and security, they might be more able to obtain and understand specific knowledge of spyware and anti-spyware programs. Also general technology familiarity helps users estimate the likelihood of new technology, and thus increase their trust of new technology. Thus, this study expects that technology familiarity is positively related to knowledge of spyware, perceived risk of spyware, and trust of anti-spyware programs.

Despite having little knowledge of spyware, individuals' general technology familiarity will increase their intention to adopt anti-spyware programs. Since past behavior is often a good predictor of future behaviors, general technology familiarity can be expected to have a direct effect on an individual's willingness to adopt anti-spyware programs (Gefen, 2000). According to Zhang (2005), the individuals' familiarity about the computer and Internet affects their behavior toward personal protection with computers. In sum, this study sets forth the following hypotheses related to general technology familiarity.

H1: General technology familiarity is positively related to knowledge of spyware.

H2: General technology familiarity is positively related to perceived risk of spyware.

H3: General technology familiarity is positively related to trust of anti-spyware programs.

H4: General technology familiarity is positively related to adoption intention.

(2) Knowledge of Spyware

When individuals have knowledge of spyware, they would feel more threatened by spyware because they would know that spyware harms computer usage by slowing computer and internet speed as well as by infringing on individuals' privacy without any permission.

This study argues that the more knowledge the user has, the stronger the perceived risk of spyware. For example, if a user only knows that spyware slows computer hardware, his or her perceived risk would be low. If the user knows that spyware can trace keystrokes, so that it can get credit card numbers, he or she should feel a higher risk of spyware. In the same vein, a user with high level knowledge on spyware would more likely to trust anti-spyware programs because anti-spyware programs are the best way to protect computers against spyware.

Based on the TRA, the *beliefs → attitudes → intentions* framework supports this study's presented arguments in terms of perceived risk and trust. Fishbein and Ajzen (1975) regarded knowledge as a belief held by individual. The belief influences an individual's positive attitude, which is partially included in trust of anti-spyware programs in the present study. According to Jasperson, Zmud, and Sambamurthy (2003), knowledge influences belief. Thus, individuals with a high level of knowledge of spyware would have negative belief (risk) of spyware and positive belief (trust) of anti-spyware programs.

In the Web behavior context, several studies concluded that the online shopping experience influenced consumer's intention to purchase products (Steven, Gerald, & Eric, 1999). Gefen et al. (2003) pointed out that with increased knowledge, intention to use systems or use online shopping increased. In the organizational context, Rogers (1995) discussed the role of knowledge in influencing persuasion, which in turn influences decision and implementation. Churchman (1971) noted that knowledge goes beyond being a collection of information and has the meaning of action and potential for action. Sveiby (1997) also referred to knowledge as "a capacity to act." Likewise consumer knowledge is a significant predictor of consumer's decision making (Zhang, 2005).

In sum, this study has the following hypotheses related to knowledge of spyware as a predictor.

H5: Knowledge of spyware is positively related to perceived risk of spyware.

H6: Knowledge of spyware is positively related to trust of anti-spyware programs.

H7: Knowledge of spyware is positively related to adoption intention.

(3) Perceived Risk of Spyware

The phrase: enemy of my enemy is my friend is very relevant to this study. Individual's negative belief about spyware would influence the positive belief and attitude about anti-spyware programs. In other words, a perceived risk of spyware will increase trust of anti-spyware program.

The proposed research model predicts that individuals engage in risk-reducing activities by adopting anti-spyware programs in order to reduce their perceived risk level.

Because of the privacy invasions by spyware, anti-spyware utilities are becoming necessary software to safeguard security (Clyman, 2004). Individuals with a negative perception of spyware will perform safety behavior to remove the danger of spyware because risks by spyware can be managed or reduced when users adopt anti-spyware programs.

According to Hu and Dinev (2007), awareness of the dangers of spyware was a direct predictor of intentions to take protective measures. Therefore, perceived risk of spyware positively influences intention to adopt anti-spyware programs. Similarly, it is possible that user's trust of anti-spyware programs might reduce the perceived risk of spyware. However, this study does not consider this casual relationship because this study focuses on the path from a user's general technology familiarity to intention to adopt anti-spyware programs. Thus, this study assumes that a user's perceived risk of anti-spyware is an antecedent of trust of anti-spyware program.

In sum, this study has the following hypotheses related to the perceived risk of spyware.

H8: Perceived risk of spyware is positively related to trust of anti-spyware programs.

H9: Perceived risk of spyware is positively related to adoption intention.

(4) Trust of Anti-Spyware Programs

In consumer-based e-commerce contexts, trusting intention represents users' intention to engage in consequent transactions with online firms (Jarvenpaa, Tractinsky, & Vitale, 2000). In the context of protective information systems, people develop trust toward adopting anti-spyware programs when they perceive it as an effective tool to enhance security and privacy of their system against spyware (Lee & Kozar, 2008). In this study, benevolence and integrity in trust partially include positive attitude (Bhattacherjee, 2002) as well as belief. Thus, trust of anti-spyware program will influence intention to adopt anti-spyware programs.

H10: Trust of anti-spyware programs is positively related to adoption intention.

(5) Hypothesis for differences between the U.S. and South Korea

Cross-country comparative study is a stream of information systems research. Several studies have found differences between countries in terms of the Internet, e-commerce, and IT awareness and adoption.

Park and Jun (2002) examined the differences in the internet usage, innovativeness on the Internet, the perceived risks of online shopping and online shopping behavior between the U.S. and South Korea. Significant differences were found in Internet usage and perceived risks of online shopping, indicating that the sample in South Korea showed longer usage of the Internet per week and higher perceived risks of usage of the Internet per week and higher perceived risks of online shopping than found in the U.S. Hwang, Jung, and Salvendy (2006) investigated online shopping preferences in three countries – the U.S., South Korea, and Turkey; and found significant cross-national differences in online shopping preferences with regard to information accuracy, security and product-price comparison.

Studies have examined the cultural differences in perceived trust in e-commerce. Jarvenpaa and Tractinsky (1999) argued that the cultural background of an online consumer is one of determinants of trust. Karvonen, Cardholm, and Karlsson (2000) tried to find out the role of cultural factors in the formation of trust on the users of e-commerce by comparing Finnish users with Swedish users and found that the differences in user's perception on security issues of e-commerce between two groups existed, but not significantly. Meanwhile, Siala, O'Keefe, and Hone (2004) examined whether religion as a cultural variable can be a factor of trust in the context of e-commerce. They found that the Muslim users showed significantly more trust in the Muslim site compared to the Christian site.

Schmidt, Johnston, Arnett, Chen, and Li (2008) investigated computer security awareness in terms of virus, spyware, and rootkit between the U.S. and China; and they found significant differences in the U.S. and Chinese user perceptions with regard to spyware and computer viruses and U.S. users had a higher self-reported knowledge of spyware and viruses.

The distinct cultural difference between the U.S. and South Korea is individualism/collectivism, defined as the "degree to which the individual emphasizes his/her own needs as opposed to the group needs and prefers to act as an individual rather than as a member of a group (Strite & Karahanna, 2006, p682). In the individualistic cultures, social behavior is mainly guided by personal goals, while in collectivistic cultures the goals of the collective have the dominant influence in shaping behavior (Triandis, 1989). In individualistic cultures, the self is regarded as separate from society and identity is determined by individual achievement rather than in terms of group membership and the position of the group in society (Hofstede, 1980). The U.S. is considered an individualistic while South Korea is considered a collectivistic culture. This study examines the differences between the U.S. and South Korea in terms of computer, Internet, and security familiarity, knowledge of spyware, perceived risk of spyware, trust of anti-spyware programs, and intention to adopt anti-spyware programs. Aforementioned constructs are regarded as anti-spyware adoption attitude in this study.

In sum, each country has different backgrounds, leading to the following hypothesis formulated for the current study.

H11: Significant differences exist in anti-spyware adoption attitude between the U.S. and South Korea.

A summary of research hypotheses and the expected direction of relationship are illustrated in Table 2-2.

Table 2-2. Summary of Research Hypotheses

Reference Number	Hypothesis	Direction of relationship
Hl	General technology familiarity is positively related to the knowledge of spyware.	+
H2	General technology familiarity is positively related to perceived risk of spyware.	+
H3	General technology familiarity is positively related to trust of anti-spyware programs.	+
H4	General technology familiarity is positively related to adoption intention.	+
H5	Knowledge of spyware is positively related to perceived risk of spyware.	+
H6	Knowledge of spyware is positively related to trust of anti-spyware programs.	+
H7	Knowledge of spyware is positively related to adoption intention.	+
H8	Perceived risk of spyware is positively related to trust of anti-spyware programs.	+
H9	Perceived risk of spyware is positively related to adoption intention.	+
H10	Trust of anti-spyware programs is positively related to adoption intention.	+
H11	Significant differences exist in anti-spyware adoption attitude between the U.S. and South Korea.	N/A

In chapter 3, the research methods used in this study are explained. Chapter 3 examines the sampling method, statistical analysis, and validation methods.

Chapter 3

Research Methodology

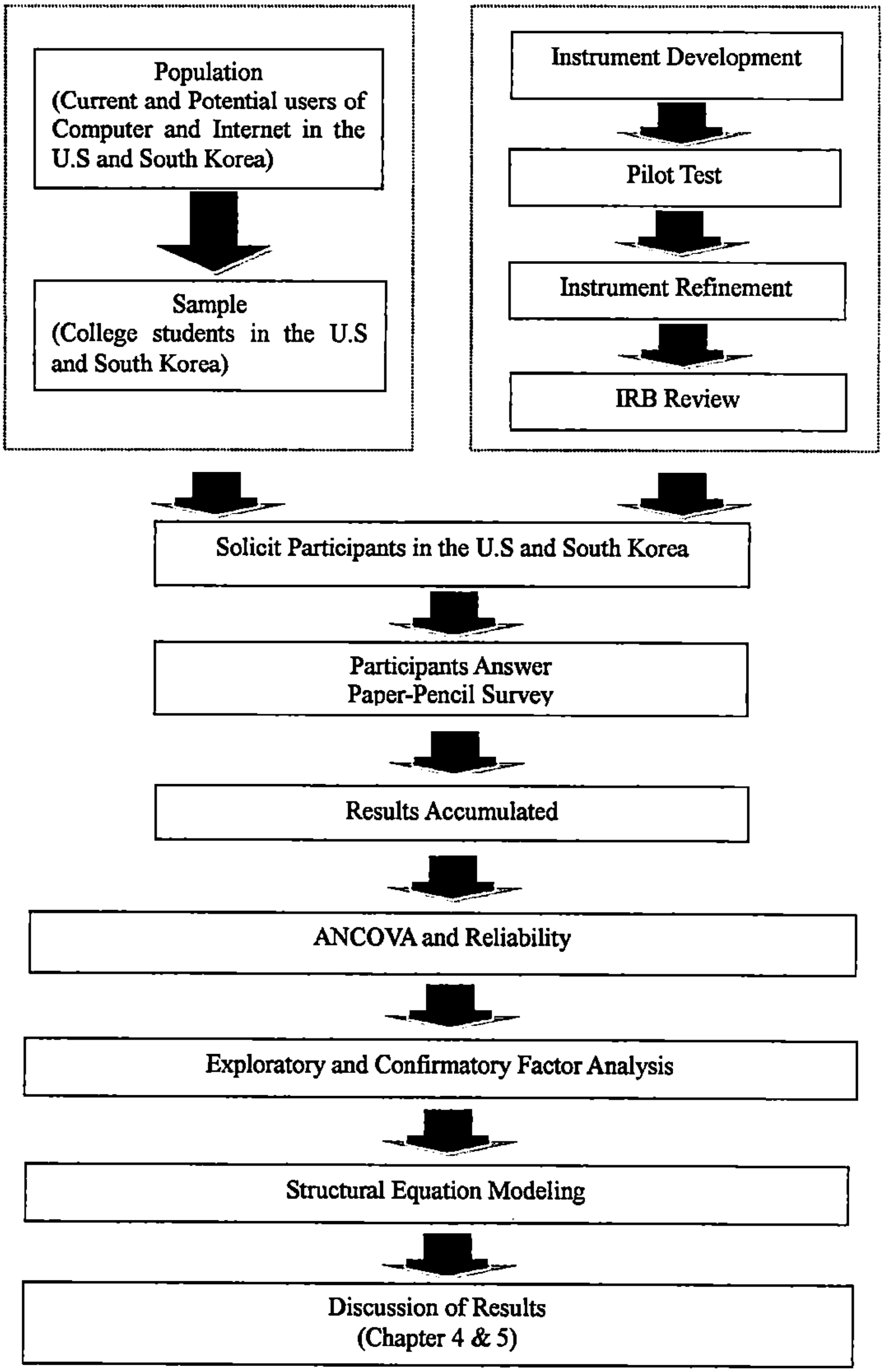
Chapter 3 discusses the research methodology. The first section will provide a brief outline of the methodology.

1. Outline of the Research Methodology

This study examined general technology familiarity and anti-spyware program adoption, utilizing an experiential exploratory survey. Figure 3-1 presents an overview of the research methodology of this study. The participants were undergraduate and graduate college students in the U.S. and South Korea.

The experiential survey was administered to college students and then measured the variables of interest to this study. The data of the surveys from two countries was collected and analyzed. The rest of this chapter provides the details about research methods, including sampling, statistical analysis, and validation methods.

Figure 3-1. Research Methodology


Population
(Current and Potential users of Computer and Internet in the U.S and South Korea)
Sample
(College students in the U.S and South Korea)
Instrument Development
Pilot Test
Instrument Refinement
IRB Review
Solicit Participants in the U.S and South Korea
Participants Answer Paper-Pencil Survey
Results Accumulated
ANCOVA and Reliability
Exploratory and Confirmatory Factor Analysis
Structural Equation Modeling
Discussion of Results
(Chapter 4 & 5)

2. Population and Sample

The target population for this study was current and potential users of the Internet in the U.S. and South Korea. The participants for this study were undergraduate and graduate students, of all level currently enrolled at both Morehead State University[2] in the U.S. and Yeungnam University[3] in South Korea. Although some bias may exist due to a convenience sampling, students are regarded as an appropriate surrogate in technology acceptance research because students are current and potential users' of anti-spyware program. McKnight et al. (2002) argued that students could be used as subjects for research that resembles the real situation, such as in the context of protective technology adoption. Thus, this study used college students as participants to develop a new model in context of protective technology acceptance.

3. Survey Instrument Development

One of objectives of this study was to develop a survey instrument to appropriately measure the dimensions of technology familiarity as well as the other constructs that comprise the proposed anti-spyware program adoption model. The instruments of the study were developed based on existing literature. The literature review identified three dimensions of general technology familiarity in

[2] This is a public university and located in Morehead, Kentucky. The university offers 78 undergraduate degree programs, including 8 associate level degrees and 12 pre-professional programs in four colleges and 20 academic departments. Enrollment for fall 2007 was 9,066.

[3] This is a private university and located in Gyeongsan, Gyeongsangbokdo. The university has 13 colleges, 71 academic departments, and 8 graduate schools. The university has 22,000 undergraduate students, 3,500 graduate students, and 1,000 faculty members and staff.

the context of protective technology adoption and examined other variables.

Items for each variable in the technology acceptance model were adopted from previous validated scales. In turn, this study modified previous scales when appropriate to ensure discriminant validity. The items were measured using a seven-point Likert scale with the highest level assigned 7 points, the middle level assigned 4 points, and the lowest level assigned 1 point. This ranking was selected to coincide with the seven-point Likert scales planned for the other survey oriented measures.

A pilot test was conducted with 83 respondents to check respondents' understanding. Next, the main test was conducted. After exploratory and confirmatory factor analysis, this study reduced the number of items to the generally accepted three to five for structural equation modeling. New variables (computer, Internet, and security familiarity) have five of the final number of items in each. The items for each variable are discussed next.

(1) General Technology Familiarity

The dimensions of general technology familiarity used for this study are computer familiarity, Internet familiarity, and security familiarity.

Schulenberg et al. (2006) developed an instrument for computer familiarity, computer aversion, and attitude. The current study adopts the items of computer familiarity of Schulenberg et al (2006). Among these items are using computer hardware and software, and reading computer magazines. For Internet familiarity, this study adopted the instruments of Spiros et al. (2005). However, another

Internet activity was added: reading articles on the Internet. Zhang (2005) measured users' security knowledge. The current study adopted and modified the instrument items of Zhang (2005). An item for general familiarity (Gefen, 2000) is included in each sub-construct as well. These sub-constructs of technology familiarity were measured by how strongly users agreed with each item. Each item of computer, Internet, and security familiarity is represented in the Tables 3-1, 3-2, and 3-3. These tables also illustrated which items were deleted in the main study based on the results of exploratory factor analysis (EFA) and confirmatory factor analysis (CFA).

Table 3-1. Source and Results of Exploratory Factor Analysis and Confirmatory Factor Analysis for Computer Familiarity Items

Code	Name	Item	Result	Source
CF1	Latest Hardware	I keep up with the latest computer hardware.	Deleted after CFA	Schulenberg et al. 2006
CF2	Changing Hardware	I am familiar with changing (installing/ upgrading) computer hardware.		Schulenberg et al. 2006
CF3	Hardware Familiarity	I am familiar with computer hardware.		Schulenberg et al. 2006
CF4	Latest Software	I keep up with the latest computer software.	Deleted after CFA	Schulenberg et al. 2006
CF5	Changing Software	I am familiar with changing (installing/ upgrading) computer software.		Schulenberg et al. 2006
CF6	Software Familiarity	I am familiar with computer software.		Schulenberg et al. 2006
CF7	Reading Magazine	I am familiar with reading computer magazines.	Deleted after EFA	Schulenberg et al. 2006
CF8	Computer Familiarity	Overall, I am familiar with computers.		Gefen, 2000

Table 3-2. Source and Results of Exploratory Factor Analysis and Confirmatory Factor Analysis for Internet Familiarity Items

Code	Name	Item	Result	Source
IF1	Search Engines	I am familiar with the use of search engines.	Deleted after CFA	Spiros et al. 2005
IF2	E-mail Use	I am familiar with the use of e-mail.		Spiros et al. 2005
IF3	Searching Information	I am familiar with searching information in Internet		Spiros et al. 2005
IF4	Purchasing Products	I am familiar with purchasing products in Internet.	Deleted after CFA	New
IF5	Reading Articles	I am familiar with reading articles in Internet.	Deleted after CFA	New
IF6	Internet Familiarity	Overall, I am familiar with Internet.		Gefen, 2000

Table 3-3. Source and Results of Exploratory Factor Analysis and Confirmatory Factor Analysis for Security Familiarity Items

Code	Name	Item	Result	Source
SF1	Privacy Violation	I am familiar with privacy violation issue.	Deleted after EFA	Zhang, 2005
SF2	Protective Knowledge	I am familiar with knowledge on protecting oneself.	Deleted after CFA	Zhang, 2005
SF3	Security Technology	I am familiar with security technology.		Zhang, 2005
SF4	Information Security	I am familiar with information security.		Zhang, 2005
SF5	Computer Security	I am familiar with computer security.		New
SF6	Internet Security	I am familiar with Internet security.		New
SF7	Security Familiarity	Overall, I am familiar with security issues.		Gefen, 2000

(2) Knowledge of Spyware

Dinev and Hu (2007) identified the construct, awareness of spyware. This study adopted and modified items designed by Dinev and Hu (2007) for the knowledge of spyware construct. This study also measured general knowledge of spyware by users (Bassellier et al. 2003). The items of knowledge of spyware are represented in Table 3-4.

Table 3-4. Source and Results of Exploratory Factor Analysis and Confirmatory Factor Analysis for Knowledge of Spyware Items

Code	Name	Item	Result	Source
KS1	Updating Knowledge	I update news and developments about the spyware technology.	Deleted after CFA	Dinev & Hu, 2007
KS2	Malicious Software	I know about the problems of malicious software intruding Internet users' computers		Dinev & Hu, 2007
KS3	Seeking Advice	I seek advice on computer web sites or magazines about anti-spyware products.		Dinev & Hu, 2007
KS4	Problem & Results	I have knowledge of spyware problems and consequences.		Dinev & Hu, 2007
KS5	Spyware Knowledge	Overall, I have general knowledge of spyware.		Bassellier et al. 2003

(3) Perceived Risk of Spyware

Workman et al. (2008) empirically tested security lapse, omission of information security, and perceived severity item in their instrument. The current study adopted and modified the instrument items developed by Workman et al. (2008). Table 3-5 displays items used in the present study to measure perceived risk of spyware.

Table 3-5. Source and Results of Exploratory Factor Analysis and Confirmatory Factor Analysis for Perceived Risk of Spyware Items

Code	Name	Item	Result	Source
PRS 1	Harm to Computers	I believe that spyware causes significant harm to my computer.	Deleted after CFA	Workman et al. 2008
PRS 2	Computer Risk	I believe that my computer is at risk if spyware is downloaded.		Workman et al. 2008
PRS 3	Personal Information	I believe that my personal information is at risk if spyware is downloaded.		Workman et al. 2008
PRS 4	Personal Privacy	I am concerned about threat to my personal privacy by spyware.	Deleted after CFA	Workman et al. 2008
PRS 5	Threat by Spyware	I am worried about threat to my computer by spyware.		Workman et al. 2008
PRS 6	Risk of Spyware	Overall, I believe that spyware is risky		Workman et al. 2008

(4) Trust of Anti-Spyware Programs

Mayer et al. (1995) conceptually examined three dimensions of trust. Bhattacherjee (2002) developed and validated trust instruments in an online shopping environment. The current study employed the instruments designed by Bhattacherjee (2002) to measure trust of anti-spyware programs. Table 3-6 displays trust items included in the current study.

Table 3-6. Source and Results of Exploratory Factor Analysis and Confirmatory Factor Analysis for Trust of Anti-Spyware Programs

Code	Name	Item	Result	Source
TA1	Ability 1	Anti-spyware programs have the skills and expertise to remove spyware.		Bhattacherjee, 2002
TA2	Ability 2	Anti-spyware programs have the ability to protect me from spyware.	Deleted after CFA	Bhattacherjee, 2002
TA3	Integrity	Anti-spyware programs are fair in its conduct of computer protection.		Bhattacherjee, 2002
TA4	Benevolence 1	Anti-spyware programs keep its users' best interest in mind during working against spyware.		Bhattacherjee, 2002
TA5	Benevolence 2	Anti-spyware programs make good-faith efforts to address most user concerns.	Deleted after CFA	Bhattacherjee, 2002
TA6	Trust	Overall, anti-spyware programs are trustworthy.		Bhattacherjee, 2002

(5) Intention to Adopt Anti-Spyware Programs

Instruments to measure adoption intention have been well developed in information systems research. This study adopts the instruments of intention to adopt anti-spyware program from two recent studies of anti-spyware program adoption. Table 3-7 shows the items.

Table 3-7. Source and Results of Exploratory Factor Analysis and Confirmatory Factor Analysis for Intention to Adopt Anti-Spyware Programs

Code	Name	Item	Result	Source
IA1	Likelihood of Use	I am likely to use anti-spyware programs.	Deleted after CFA	Lee & Kozar, 2008
IA2	Prediction of Use	I predict that I will adopt anti-spyware programs.		Lee & Kozar, 2008
IA3	Intention to Use	I intend to periodically use anti-spyware program to protect my computer from spyware.		Dinev & Hu, 2007
IA4	Recommending to Others	I will recommend to others that they use anti-spyware programs.		Dinev & Hu, 2007
IA5	Multiple Use	I will use two or more anti-spyware programs if helpful.	Deleted after CFA	New

4. Pilot Test

The pilot test was conducted to help refine wording, test validation, and eliminate potential problems in the survey instrument. After drafting the initial survey, one professor, two staff (a research associate and a librarian), and five masters students examined the survey in terms of wording, understanding, and content validity. In turn, the pilot test was administered to undergraduate students in four classes to test initial validity and reliability as well as to identify ambiguity in item wording.

Based on the English survey, the researcher, a native Korean, translated the survey instrument to Korean. To employ common and well-known terms for scholarly fields and real world, an English-Korean dictionary, Korean scholarly articles, Korean portal sites and Web pages, and Korean newspapers were used.

Next one doctoral student, one information technology specialist, one masters student and one journalist examined the survey to clarify wording and understanding. After examining the Korean survey, the reviewers compared

English and Korean. Some pointed out two technical terms which Korean students might have difficulty understanding: keystroke and denial of service (DOS) attack. Although Korean Web sites, scholarly articles, and newspapers use the terms directly, the Korean survey uses explanatory notes to clarify these terms. Finally, six people similar to the respondents were requested to note ambiguity in terms of wording and understanding. The respondent validation group responded that all of the survey items were understandable.

5. Procedure for Main Study

Structural Equation Modeling is a large-sample technique. Because sample size is an important issue in research, this study used a sample size which exceeds the recommended minimum case-per-variable ratio of five observations per item (Hair, Tatham, Anderson, & Black, 1998). Therefore, this study examined at least 200 subjects in each country.

The study used a paper-based survey. The researcher asked instructors to administer the survey in various classes at universities in the U.S. and South Korea. In each class, students, who are at least 18 years old, were solicited to participate in the survey. The same procedure was used in a middle size university in the U.S. and a large size university in South Korea. The collected data from the survey was screened to provide clean data for the testing of the main research model.

7. Data Analysis

Using SPSS 16.0, the responses from the survey were coded into a data file for statistical analyses. When two or more invalid and incomplete responses were found in each subject, all responses from subjects were dropped. One missing data in one variable was operated by using mean value. The basic information from the participants (i.e. demographics, usages for anti-spyware programs, and computer and Internet experience) were then analyzed.

8. Statistics for Main Study[4]

This study utilized four main statistics to analyze the data: analysis of covariance (ANCOVA), exploratory factor analysis (EFA), confirmatory factor analysis (CFA), and structural equation modeling (SEM). For this study, SPSS 16.0 for EFA and ANCOVA and AMOS 16.0 for CFA and SEM were used.

(1) Analysis of Covariance (ANCOVA)

Because this study compared two countries, ANCOVA was first conducted to determine if the differences between the U.S. and South Korea regarding each constructs were, in fact, significant. Gender, age, major, and classification were chosen as control variables.

[4] The summary of statistics being used is based on Kline (2005), and several dissertations and journal articles.

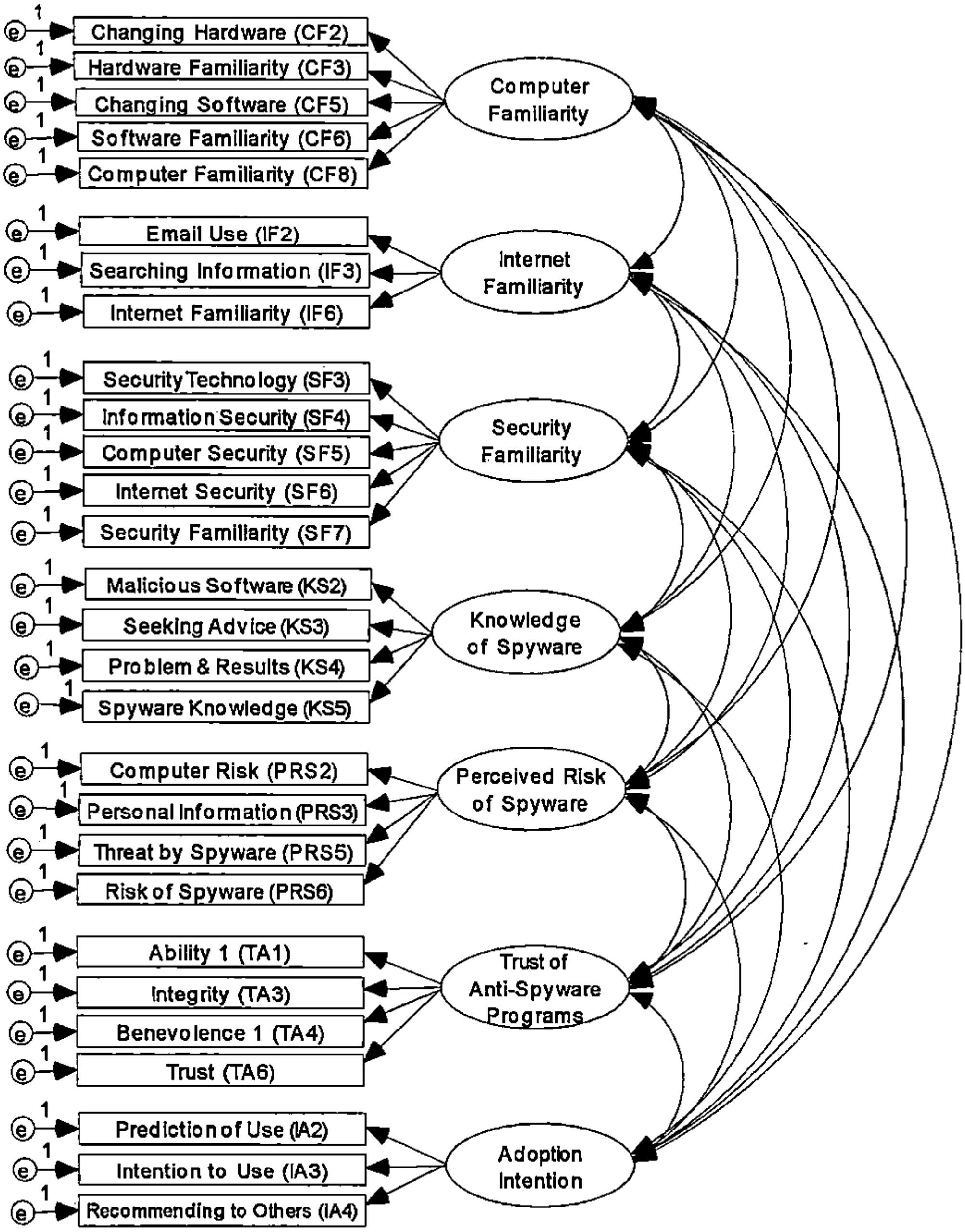
(2) Exploratory Factor Analysis (EFA)

Although the survey instruments were derived from previous studies, the instruments were modified based on the purpose of the present study. Also, this study compares the U.S. with South Korea. Therefore, EFA examines if each item is included in the factors which the study wants to measure. In turn, principle components analysis and a Varimax rotation method were used. Factor loadings of 0.5 or greater are considered practically significant and used for this study (Hair et al. 1998).

(3) Confirmatory Factor Analysis (CFA)

CFA was employed for testing the measurement model. In contrast to exploratory factor analysis, where all loadings are free to vary, CFA allows for the explicit constraint of certain loadings to be zero. In the measurement model, this study tested convergent validity, internal consistency, composite reliability, and discriminant validity. The measurement model for CFA is presented in figure 3-2.

Figure 3-2. Measurement Model (Confirmatory Factor Analysis)



(4) Structural Equation Modeling (SEM)

The main objectives of SEM are to test and estimate causal relationships using a combination of statistical data and qualitative causal assumptions (Pearl, 2000). SEM encourages confirmatory rather than exploratory modeling, and thus it is good for theory testing rather than theory building. In SEM, the qualitative causal assumptions are represented by the missing variables in each equation, as well as vanishing covariances among some error terms.

This study focuses on the relationships among several latent variables, and thus SEM is a proper analysis to help meet the research objectives. SEM has many advantages over older generation multivariate analyses (Byrne, 2001): (1) SEM allows a confirmatory approach, such as in the case of theory testing, (2) researchers can assess or correct for measurement error, (3) data analyses using SEM procedures can incorporate latent (unobserved) and observed variables, (4) SEM provides methods for modeling multivariate relations (multiple independent and dependent variables) and for estimating point and/or interval indirect effects. In turn, SEM provides a more accurate interpretation of the model. Based on the literature review and expected relationships developed in chapter 2, a path diagram expressing the causal relationships to be tested by SEM is presented in Figure 3-3.

Figure 3-3. Structural Equation Model

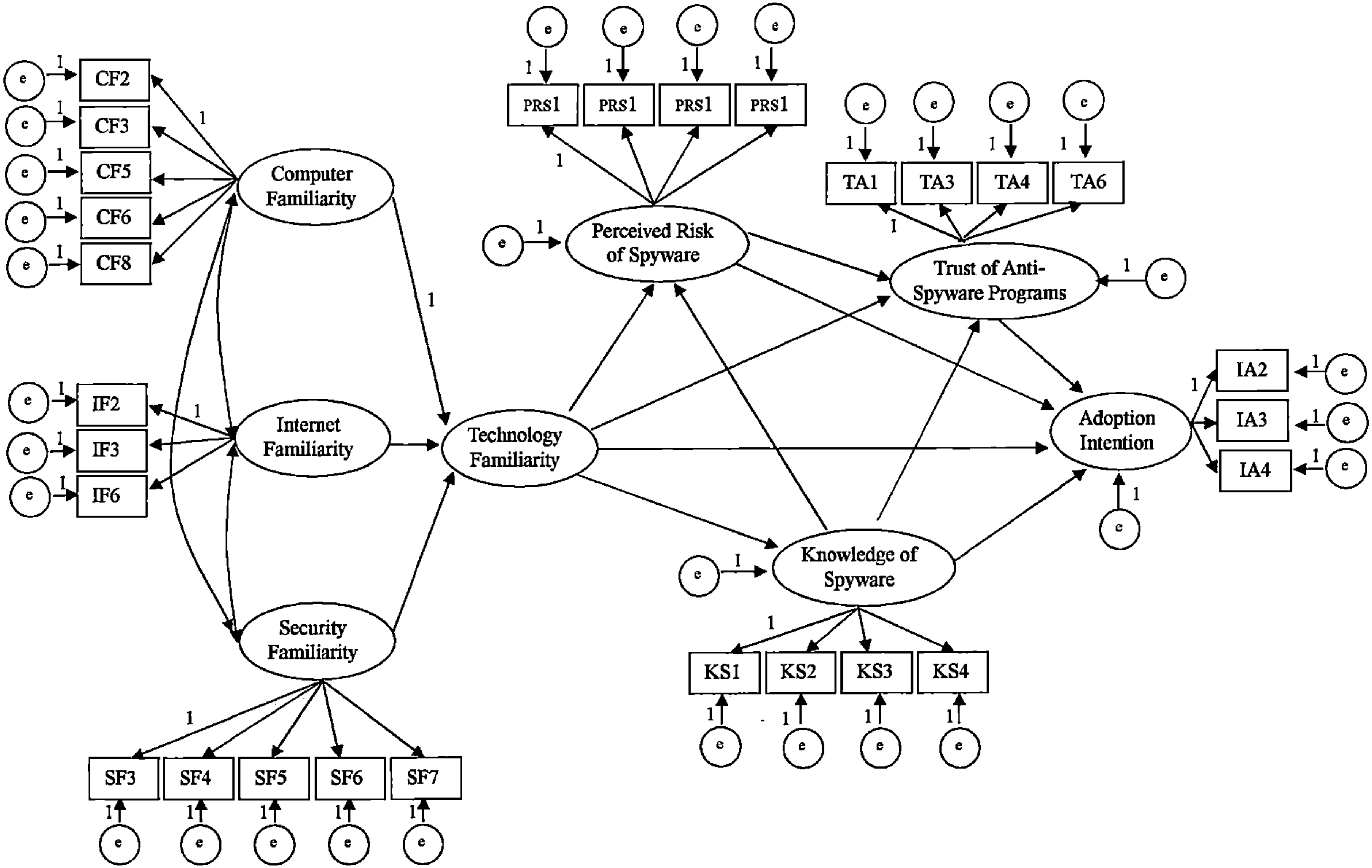


Table 3-8 is the summary of statistics being used to test each hypothesis

Table 3-8. Summary of Statistics for Hypotheses

H	Explanation	Statistics
Hl	General technology familiarity is positively related to the knowledge of spyware.	SEM
H2	General technology familiarity is positively related to perceived risk of spyware.	SEM
H3	General technology familiarity is positively related to trust of anti-spyware programs.	SEM
H4	General technology familiarity is positively related to adoption intention.	SEM
H5	Knowledge of spyware is positively related to perceived risk of spyware.	SEM
H6	Knowledge of spyware is positively related to trust of anti-spyware programs.	SEM
H 7	Knowledge of spyware is positively related to adoption intention.	SEM
H8	Perceived risk of spyware is positively related to trust of anti-spyware programs.	SEM
H9	Perceived risk of spyware is positively related to adoption intention.	SEM
H10	Trust of anti-spyware programs is positively related to adoption intention.	SEM
H11	Significant differences exist in anti-spyware adoption attitude between the U.S. and South Korea.	ANCOVA

First, the differences between the U.S. and South Korea are identified according to the results of the ANCOVA and descriptive analysis. Next, the measurement model is tested by CFA and revised. In turn, each hypothesis is examined according to the results of the SEM, and the structural model was revised according to MI (modification index). The significance and strength of the proposed relationships are investigated to determine if each hypothesis is supported. In turn, the significance and the factors of differences are inspected. Chapters 4 and 5 provide the detailed results and discussion of the results.

Chapter 4
Results

Chapter 4 describes the results of the statistical analysis, including data screening, descriptive statistics, and an examination of the measurement and structural models.

1. Data Screening

The author administered the instrument in the U.S., while a well-educated administrator administered the survey instruments in South Korea in November, 2008. Students enrolled in selected classes at the U.S. and South Korean universities were asked to fill out a paper survey during class time. Using convenience sampling, the response rates in both countries were 100 percent.

Over a period of three weeks, a total of 696 students (360 in the U.S. and 336 in South Korea) participated in the survey. Surveys with more than two missing values for one construct were eliminated. The cases that had single items missing per construct were treated with the item mean substitution method in SPSS, method for treating Likert-type scale missing data (Downey & King, 1998). This study had 686 usable responses.

2. Demographic Information

Descriptive statistics of participants showed gender, age, major and classification. The U.S. sample included 40.1% male and 59.9% female, while the South Korean sample included 50.8% male and 49.2% female. The majority of participants were aged from 18 to 27 (U.S: 93.6% and South Korea: 99.1%), the age range typical of a traditional university student. Seven percent of participants majored in computer science and computer information systems, 8.1% business related, and 84.8% were others in the U.S; 6.7% business students and 93.3% were others in South Korea. U.S results reported 43.4% freshmen, 17.4% sophomore, 16.0% junior, 19.1% senior, and 2.5% graduate students; South Korea showed 22.5% freshmen, 28.9% sophomore, 27.4% junior, 19.1% senior, and 2.1% graduate students. The demographics in both the U.S. and South Korea were analyzed and are presented in Table 4-1.

Table 4-1. Demographic Profile of the Survey Respondents

Variable	Category	U.S (%) N=357 (100)	South Korea (%) N= 329 (100)	Total 686 (100)
Gender	Male	143 (40.1)	167 (50.8)	310 (45.2)
	Female	214 (59.9)	162 (49.2)	376 (54.8)
Age	18-27	334 (93.6)	326 (99.1)	660 (96.0)
	28-35	19 (5.3)	-	19 (3.0)
	>35	4 (1.1)	3 (0.8)	7 (1.0)
Classification	Freshman	155 (43.4)	74 (22.5)	229 (33.4)
	Sophomore	62 (17.4)	95 (28.9)	157 (22.9)
	Junior	57 (16.0)	90 (27.4)	147 (21.4)
	Senior	74 (20.7)	63 (19.1)	137 (20.0)
	Graduate	9 (2.5)	7 (2.1)	16 (2.3)
Major	CS/CIS	25 (7.0)	-	25 (3.6)
	Engineering	8 (2.2)	63 (19.1)	71 (10.3)
	Business	29 (8.1)	22 (6.7)	51 (7.4)
	Others	295 (82.6)	244 (74.2)	539 (78.6)

The participants were asked to answer questions related to computer usage including spyware usage, operating systems, and time spent using computer and the Internet. The majority of participants (66.9% in U.S and 52.6% in South Korea) used anti-spyware programs. Thirty-one percent in the U.S and 42.9% in South Korea used one anti-spyware program, and 25.4% in the U.S and 23.7% in South Korea used two or more anti-spyware programs. This study also asked how much was spent on the computer and Internet. Overall, 62.5% of participators in the U.S and 65% in South Korea spent from one to five hours using the computer each day; 77.6% of respondents in the U.S and 80.9% of South Korean respondents for Internet use. Usages for anti-spyware programs, computer, and Internet are presented in Table 4-2.

Table 4-2. Anti-Spyware Program, Computer, and Internet Usage

Variable	Category	U.S (%) N=357	South Korea (%) N=329	Total N=686
Anti-spyware program Use	Yes	239 (66.9)	173 (52.6)	412 (60.1)
	No	41 (11.5)	95 (28.9)	136 (19.8)
	Not sure	77 (21.6)	61 (18.5)	138 (20.1)
Number of anti-spyware programs used	1	110 (34.1)	118 (42.9)	228 (33.2)
	2	29 (18.3)	56 (20.4)	85 (12.4)
	>3	23 (7.1)	9 (3.3)	32 (4.7)
	Not sure	131 (40.6)	92 (33.5)	223 (32.5)
O.S. (multiple responses)	Windows XP	209 (59)	277 (84.2)	486 (70.8)
	Windows Vista	176 (49)	49 (14.9)	225 (32.8)
	Others	29 (8)	7 (2.1)	36 (5.2)
Time spent using Computer	Less than 1 hour	112 (31.4)	100 (30.4)	212 (30.9)
	1 up to 2 hours	118 (33.1)	110 (33.4)	228 (33.2)
	2 up to 3 hours	59 (16.5)	69 (21.0)	128 (18.7)
	3 up to 4 hours	27 (7.6)	25 (7.6)	52 (7.6)
	4 up to 5 hours	19 (5.3)	10 (3.0)	29 (4.2)
	5 hours more	22 (6.2)	15 (4.6)	37 (5.4)
Time spent using Internet	Less than 1 hour	44 (12.3)	48 (14.6)	92 (13.4)
	1 up to 2 hours	132 (37.0)	127 (38.6)	259 (37.8)
	2 up to 3 hours	82 (23.0)	96 (29.2)	178 (25.9)
	3 up to 4 hours	35 (9.8)	27 (8.2)	62 (9.0)
	4 up to 5 hours	28 (7.8)	16 (4.9)	44 (6.4)
	5 hours more	32 (9.0)	15 (4.6)	47 (6.9)

3. Measurement Model

Descriptive statistics, as well as exploratory factor analysis and confirmatory factor analysis were used to examine and refine the measurement model. The measurement model was used to evaluate the validity and reliability of the items.

(1) Descriptive Statistics and ANCOVA

Descriptive statistics (mean and standard deviation) of the measurement scales were identified. Each of the items were measured by a seven-point Likert-type scale ranging from 1 (strongly disagree) to 7 (strongly agree). The higher the mean score, the more the respondent agreed with the item. The lower the score, the more the individual disagreed with the statement.

Analysis of covariance was also conducted for testing H11. For ANCOVA, this study used four control variables: gender, major, age, and classification. Every construct (computer familiarity, Internet familiarity, security familiarity, knowledge of spyware, perceived risk of spyware, trust of anti-spyware programs, and intention to adopt anti-spyware programs) was examined by ANCOVA.

In statistics, p-values of every construct significantly differed at the 0.05 level. Thus, the results supported H11. The descriptive statistics and the results of ANCOVA are showed in Appendix A; and the results are discussed in the conclusion.

(2) Reliability Test

Two types of reliability tests were conducted, using standardized Cronbach's alpha: split half reliability and interrater reliability.

Split half reliability randomly splits the data set into two. A score for each participant is then calculated based on each half of the scale. If a scale is very reliable, a person's score on one half of the scale should be the same or similar to their score on the other half. This study had acceptable results from split half reliability test in the U.S. and South Korea (See table 4-3).

This study used two languages for the questionnaire, which asked the same questions. Also, the results were significantly different between the U.S and South Korea. Thus, interrater reliability was tested. Each construct had affordable results for comparison, 0.913 to 0.961 in U.S and 0.869 to 0.948 in South Korea. The results are in Table 4-3.

Table 4-3. Reliability Test

Variables	# items	Standardized item alpha						
		U.S.			South Korea			Total N=686
		First Half N=179	Second Half N=178	Total N=357	First Half N=165	Second Half N=164	Total N=329	
Computer Familiarity	8	.935	.934	.934	.926	.932	.929	.932
Internet Familiarity	6	.925	.877	.906	.889	.881	.885	.902
Security Familiarity	7	.972	.973	.972	.930	.929	.930	.961
Knowledge of Spyware	5	.936	.934	.935	.903	.918	.911	.927
Perceived Risk of spyware	6	.970	.949	.960	.940	.944	.942	.952
Trust of anti-spyware programs	6	.955	.933	.945	.944	.924	.935	.945
Intention to Adopt Anti-Spyware Programs	5	.955	.940	.948	.923	.919	.921	.938

(3) Exploratory Factor Analysis

Exploratory factor analysis was used to identify whether the correlations between a set of indicators stem from their relationship to one or more constructs in the data. Seven of the proposed constructs that have been drawn from and modified from previous studies were examined with a principal components factor analysis using a Varimax rotation. However, CF7 (Reading Magazine) was less than 0.5 in the U.S. (0.479) and South Korea (0.499); and SF1 (Privacy Violation) was less than 0.5 in South Korea (0.437). After dropping CF7 and SF1, a second factor analysis was done. Kaiser-Meyer-Olkin (KMO) is the test to assess the appropriateness of using factor analysis on data. KMO is 0.949 in the U.S. and, 0.917 in South Korea, which means highly acceptable. The results of first and second exploratory factor analysis are showed in Appendix B.

(4) Confirmatory Factor Analysis (CFA)

This study tested the research model through Structural Equation Modeling (SEM) using AMOS 16.0 for Windows. The covariance structural model consists of two parts: the measurement model, and the structural model. Following Anderson and Gerbing (1988), the model was tested using a two-stage approach: (1) confirmatory factor analysis (CFA) to evaluate construct validity regarding convergent and discriminant validity, and (2) structural equation modeling to test the hypotheses. The CFA and SEM examined goodness of fit, checking possible improvement (MI: modification indices), and interpreting the results.

Several indices to measure goodness of fit were used in this study. They are presented in the Table 4-4.

Table 4-4. Fit Indices Used in this Study (Modified from Kline, 2005)

Fit Index		Description	Desired Level
Absolute Fix Indexes	χ^2 (Chi-Square)	- Known as likelihood ratio chi-square or generalized likelihood ratio (sensitive to sample size) - The discrepancy between the unrestricted sample covariance matrix and the restricted covariance matrix	Smaller
	χ^2/df	- Called the Normed chi-square - The chi-square fit index divided by degrees of freedom to reduce the sensitivity to sample size	<3.0
	GFI (Goodness of Fit Index)	- The very first standardized fit index (Jöreskog & Sörbom, 1981) and originally associated with LISREL - Analogous to a squared multiple correlation (R2), but the GFI is a matrix proportion of explained variance.	>0.9
	AGFI (Adjusted Goodness of Fit Index)	- Adjusted by the ratio of degrees of freedom for the proposed model to the degrees of freedom for the null model - Correcting downward the value of the GFI based on model complexity.	>0.8
	RMR (Root Mean Square Residual)	- A measure of the mean absolute value of the covariance residuals.	<0.05
Parsimony-Adjusted Index	RMSEA (Root Mean Square Error of Approximation)	- Explaining the error of approximation in the population	<0.05: good fit 0.05-0.08: acceptable fit
Incremental Fit Indexes	NFI (Normed Fit Index)	- Statistics between zero and one that compare the proposed model to the null model - Sample based	>0.90
	NNFI (=TLI) (Non-Normed Fit Index)	- Sample based and parsimony adjusted	>0.90
	CFI (Comparative Fit Index)	- Originally associated with EQS - Value (0-1) are derived from the comparison of a hypothesized model with the null model	>0.90

(5) Measurement Model Fit

The first confirmatory factor analysis examined the seven constructs with 41 items included in the research model and previously examined with exploratory factor analysis. Table 4-5 shows mixed results for the fit of measurement model. Goodness of Fit Index was below the recommended values of 0.90 (Gefen et al. 2000) in the U.S (0.796) and South Korea (0.772). Adjusted Goodness of Fit Index was also below the value of 0.80 in the U.S. (0.768) and South Korea (0.742). In both countries, Normed Fit Index was lower than the expected value of 0.90. Non-Normed Fit Index was acceptable in the U.S. (0.927), but not in South Korea (0.898). Comparative Fit Index was acceptable in both.

These model fit results indicated that the measurement model is poor. To improve overall model fit for both countries, this study dropped thirteen items[5] because of a lower than 0.70 of standardized factor loading (Hair et al. 1998), and high modification index which indicates high error correlation. 0.70 is minimum value of recommended standardized factor loading (Hair et al. 1998). After conducting the second confirmatory factor analysis, Adjusted Goodness of Fit Index, Root Mean Square Error of Approximation, Normed Fit Index, Non-Normed Fit Index, and Comparative Fit Index were found acceptable for the U.S. and South Korea; therefore, the second model had a highly improved model fit. Although Goodness of Fit Index and Root Mean Square Residual did not have desired fit levels, this study assumed that the measurement model is good in the U.S. and South Korea. The Goodness of Fit indices of the initial model and

[5] Dropped are CF1, CF4, IF1, IF4, IF5, SF2, KS1, PRS1, PRS4, TA2, TA5, IA1, and IA5.

revised model are presented in Table 4-5.

Table 4-5. Goodness of Fit indices for the Measurement Model

	Initial Model		Revised Model		Desired Level
	U.S	South Korea	U.S	South Korea	
Total Number of Items	41		28		
χ^2	1860.048	1960.348	648.733	817.112	Smaller
df	758	758	329	329	-
χ^2/df	**2.454**	**2.586**	**1.972**	**2.484**	<3.0
GFI	.796	.772	.887	.843	>0.9
AGFI	.768	.741	**.861**	**.807**	>0.8
RMR	.096	.110	.075	.088	<0.05
RMSEA	**.064**	**.070**	**.052**	**.067**	<0.08
NFI	.892	.856	**.943**	**.909**	>0.90
NNFI	**.927**	.898	**.967**	**.935**	>0.90
CFI	**.933**	**.906**	**.971**	**.944**	>0.90

(6) Unidimensionality and Convergent Validity

The confirmatory factor analysis (CFA) was completed with maximum likelihood estimation. CFA allows the a priori specification of the relationships between the latent variables and their indicators. Unidimensionality and convergent validity ensure that all items measure a single underlying construct (Bagozzi & Fornell, 1982). Modifications were based on factor loadings and modification indices. Standardized factor loadings were expected to meet the minimum recommended value of 0.70, which indicate that the indicator reliability is over 0.50 (Hair et al. 1998), thus items with lower than 0.7 standardized factor loading were dropped. Factor loading and squared multiple correlation for each variable follow.

a. Computer Familiarity

After dropping CF7 (Reading Magazine) from EFA, seven indicators remained to measure computer familiarity. The t-values were significant at the 0.05 level. CF1 (Latest Hardware) and CF4 (Latest Software) were dropped because of their contents asking about practical behavior and CF1 was lower than 0.7 in South Korea. The values for the standardized factor loadings, which determine the relative importance of the observed variables as indicators of computer familiarity, showed relatively high loadings ranging from 0.811 to 0.913 in U.S and 0.808 to 0.904 in South Korea. The squared multiple correlation (SMC) refers to the extent to which the indicator explains the variable, which is similar to R^2 in the regression model. SMC ranged from 0.658 to 0.834 and 0.653 to 0.816 in the U.S and South Korea, respectively. The results of computer familiarity are presented in Table 4-6.

Table 4-6. Factor Loading and Squared Multiple Correlation of Computer Familiarity

Item	U.S		South Korea	
	Factor Loading	SMC	Factor Loading	SMC
Changing Hardware (CF2)	0.854	0.729	0.880	0.774
Hardware Familiarity (CF3)	0.873	0.763	0.893	0.797
Changing Software (CF5)	0.883	0.780	0.904	0.816
Software Familiarity (CF6)	0.913	0.834	0.898	0.807
Computer Familiarity (CF8)	0.811	0.658	0.808	0.653

Table 4-7. Scale Refinement of Computer Familiarity

Nation	Items	# items	df	χ^2	p	χ^2/df	RMSEA	GFI	AGFI	CFI
U.S	CF1…6, 8	7	14	244.210	0.000	17.444	0.215	0.859	0.719	0.900
	CF2,3,5,6,8	5	5	65.161	0.000	13.032	0.184	0.941	0.822	0.962
South Korea	CF1…6, 8	7	14	273.069	0.000	19.505	0.238	0.827	0.653	0.877
	CF2,3,5,6,8	5	5	123.732	0.000	24.746	0.269	0.864	0.593	0.926

(1) The initial model does not show satisfactory results. Modification index (U.S.: 121.45, South Korea: 71.032) indicated a high error correlation between CF1 and CF4. Both CF1 and CF4 were dropped because of their contents asking about practical behavior.

b. Internet Familiarity

Six indicators were used to measure Internet familiarity. The t-values were significant at the 0.05 level. IF1 (Search Engines) in both countries, IF4 (Purchasing Products) in the U.S., and IF5 (Reading Articles) in South Korea were lower than 0.7 of factor loading and thus dropped. After dropping three items, a second CFA was conducted. Standardized factor loadings ranged from 0.869 to 0.920 in the U.S and 0.742 to 0.861 in South Korea. Squared multiple correlation ranged from 0.755 to 0.846 and 0.551 to 0.741 in the U.S and South Korea, respectively. The results of Internet familiarity are showed in Table 4-8.

Table 4-8. Factor Loading and Squared Multiple Correlation of Internet Familiarity

Item	U.S		South Korea	
	Factor Loading	SMC	Factor Loading	SMC
Email Use (IF2)	.869	0.755	.742	0.551
Searching Information (IF3)	.920	0.846	.861	0.741
Internet Familiarity (IF6)	.900	0.811	.832	0.693

Table 4-9. Scale Refinement of Internet Familiarity

Nation	Items	# items	df	χ^2	p	χ^2/df	RMSEA	GFI	AGFI	CFI
U.S	IF1... IF6	6	9	45.725	0.000	5.081	0.049	0.956	0.898	0.975
	IF2, 3, 6	4	0							
South Korea	IF1... IF6	6	9	52.792	0.000	5.866	0.063	0.941	0.861	0.958
	IF2, 3, 6	4	0							

(1) In the U.S. high error correlation was found between IF4 and IF5 (MI: 20.179) and between IF3 and IF4 (MI: 15.008). In South Korea, high error correlation was found between IF1 and IF3 (16.200) and between IF5 and IF6 (MI15.410).

(2) Although the model shows satisfactory fit, IF1, IF4, and IF5 were dropped because of low factor loading: IF1 (U.S.: 0.677, South Korea: 0.685), IF4 (U.S.: 0.585), and IF5 (South Korea: 0.690)

(3) Statistical fit cannot be obtained from only three items (0 of degree of freedom).

c. Security Familiarity

After dropping SF1 (Privacy Violation) from EFA, six items remained to measure security familiarity. The t-values were significant at the 0.05 level. High error correlation was found between SF2 (Protective Knowledge) and SF3 (Security Technology) and between SF2 (Protective Knowledge) and SF5 (Computer Security) in both countries. Thus, SF2 was dropped in the interest of parsimony. After dropping SF2, standardized factor loadings were high, ranging from 0.914 to 0.951 in the U.S and 0.871 to 0.937 in South Korea. Squared multiple correlation ranged from 0.835 to 0.905 and 0.759 to 0.877 in the U.S and South Korea, respectively. The results of security familiarity are presented in Table 4-10.

Table 4-10. Factor Loading and Squared Multiple Correlation of Security Familiarity

Item	U.S		South Korea	
	Factor Loading	SMC	Factor Loading	SMC
Security Technology (SF3)	.929	0.863	.871	0.759
Information Security (SF4)	.939	0.882	.930	0.864
Computer Security (SF5)	.951	0.905	.937	0.877
Internet Security (SF6)	.914	0.835	.918	0.843
Security Familiarity (SF7)	.947	0.896	.915	0.838

Table 4-11. Scale Refinement of Security Familiarity

Nation	Items	# items	df	χ^2	p	χ^2/df	RMSEA	GFI	AGFI	CFI
U.S	SF2...SF7	6	9	96.518	0.000	10.724	0.165	0.916	0.804	0.972
	SF3...SF7	5	5	49.410	0.000	9.882	0.158	0.946	0.839	0.982
South Korea	SF2...SF7	6	9	116.048	0.000	12.894	0.190	0.880	0.721	0.952
	SF3...SF7	5	5	89.239	0.000	17.848	0.227	0.898	0.694	0.958

(1) High error correlation was found between SF2 and SF3 (U.S.:33.375, South Korea: 19.826) and between SF2 and SF5 (U.S.: 10.944, South Korea: 15.785) so that SF2 was dropped in the interest of parsimony.

d. Knowledge of Spyware

Five items were used to measure knowledge of spyware. The t-values were significant at the 0.05 level. KS1 (Updating Knowledge) was dropped because of its low factor loading in South Korea, and because MI showed a high error correlation between KS1 (Updating Knowledge) and KS2 (Malicious Software). After dropping KS1, standardized factor loadings ranged from 0.798 to 0.953 in the U.S and 0.774 to 0.948 in South Korea. Squared multiple correlation ranged from 0.637 to 0.908 in the U.S. and 0.599 to 0.898 in South Korea. The results of knowledge of spyware are analyzed in Table 4-12.

Table 4-12. Factor Loading and Squared Multiple Correlation of Knowledge of Spyware

Item	U.S		South Korea	
	Factor Loading	SMC	Factor Loading	SMC
Malicious Software (KS2)	0.860	0.740	0.780	0.608
Seeking Advice (KS3)	0.798	0.637	0.774	0.599
Problem & Results (KS4)	0.921	0.849	0.948	0.898
Spyware Knowledge (KS5)	0.953	0.908	0.921	0.848

Table 4-13. Scale Refinement of Knowledge of Spyware

Nation	Items	# items	df	χ^2	p	χ^2/df	RMSEA	GFI	AGFI	CFI
U.S	KS1...KS5	5	5	38.099	0.000	7.620	0.136	0.963	0.888	0.979
	KS2...KS5	4	2	8.594	0.014	4.297	0.096	0.995	0.985	0.995
South Korea	KS1...KS5	5	5	16.606	0.000	3.321	0.084	0.980	0.939	0.990
	KS2...KS5	4	2	0.4	0.819	0.2	0.000	0.999	0.997	1

(1) Although the initial model shows satisfactory fit, KS1 was dropped because of its low factor loading in South Korea (0.660), and because MI (16.562) showed a high error correlation between KS1 and KS2.

e. Perceived Risk of Spyware

Six items were used to measure perceived risk of spyware. The t-values were significant at the 0.05 level. For parsimony of measurement model, PRS1 (Harm to Computers) and PRS4 (Personal Privacy) were dropped. In the second CFA, standardized factor loadings were high, ranging from 0.850 to 0.949 in the U.S and 0.853 to 0.912 in South Korea. Squared multiple correlation ranged from 0.723 to 0.901 and 0.727 to 0.831 in the U.S and South Korea, respectively. The results of perceived risk of spyware are presented in Table 4-14.

Table 4-14. Factor Loading and Squared Multiple Correlation of Perceived Risk of Spyware

Item	U.S		South Korea	
	Factor Loading	SMC	Factor Loading	SMC
Computer Risk (PRS2)	.935	0.875	.875	0.766
Personal Information (PRS3)	.949	0.901	.881	0.776
Threat by Spyware (PRS5)	.850	0.723	.853	0.727
Risk of Spyware (PRS6)	.917	0.841	.912	0.831

Table 4-15. Scale Refinement of Perceived Risk of Spyware

Nation	Items	# items	df	χ^2	p	χ^2/df	RMSEA	GFI	AGFI	CFI
U.S	PRS1...PRS6	6	9	139.183	0.000	15.465	0.202	0.891	0.747	0.948
	PRS2, 3, 5, 6	4	2	17.18	0.000	8.590	0.146	0.977	0.887	0.990
South Korea	PRS1...PRS6	6	9	189.277	0.000	21.031	0.247	0.845	0.638	0,905
	PRS2, 3, 5, 6	4	2	39.051	0.000	19.525	0.238	0.939	0.697	0.967

(1) Initial model does not show satisfactory model fit. MI indicated high error correlations between PRS1 and PRS2 (U.S.: 29.878, South Korea: 56.197) and between PRS4 and PR5 (U.S.: 53.396, South Korea: 27.566). PRS1 and PRS4 were dropped in the interest of parsimony.

f. Trust of Anti-Spyware Programs

Six items were used to measure trust of anti-spyware programs. The t-values were significant at the 0.05 level. TA2 (Ability 2) and TA5 (Benevolence 2) were removed in the interest of parsimony of the study. After dropping two items, standardized factor loadings ranged from 0.784 to 0.933 in the U.S and 0.782 to 0.916 in South Korea. Squared multiple correlation ranged from 0.614 to 0.871 and 0.612 to 0.839 in the U.S and South Korea, respectively. The results of trust of anti-spyware programs are listed in Table 4-16.

Table 4-16. Factor Loading and Squared Multiple Correlation of Trust of Anti-Spyware Programs

Item	U.S		South Korea	
	Factor Loading	SMC	Factor Loading	SMC
Ability 1 (TA1)	.784	0.614	.801	0.642
Integrity (TA3)	.933	0.871	.916	0.839
Benevolence 1 (TA4)	.860	0.739	.782	0.612
Trust (TA6)	.875	0.766	.796	0.634

Table 4-17. Scale Refinement of Trust of Anti-Spyware Programs

Nation	Items	# items	df	χ^2	p	χ^2/df	RMSEA	GFI	AGFI	CFI
U.S	TA1...TA6	6	9	110.766	0.000	12.307	0.178	0.907	0.783	0.949
	TA1, 3, 4, 6	4	2	24.575	0.000	12.287	0.178	0.968	0.848	0.980
South Korea	TA1...TA6	6	9	117.162	0.000	13.018	0.191	0.880	0.720	0.934
	TA1, 3, 4, 6	4	2	9.760	0.008	4.880	0.109	0.985	0.924	0.990

(1) MI indicated high error correlations between TA1 and TA2 (U.S.: 24.638, South Korea: 30.369) and between TA3 and TA5 (U.S.: 18.349, South Korea: 6.999). TA5 also had high error correlations with TA4 (MI: 21.798) and TA6 (MI: 43.128) in South Korea. Thus, TA2 and TA5 were dropped in the interest of parsimony.

g. Intention to Adopt Anti-Spyware Programs

Five items were used to measure intention to adopt anti-spyware programs. The t-values were significant at the 0.05 level. IA5 (Multiple Use) was dropped because of lower than 0.7 of standardized factor loading in South Korea. Also, IA1 (Likelihood of Use) was removed for parsimony of the study. Standardized factor loadings ranged from 0.856 to 0.957 in the U.S and 0.836 to 0.949 in South Korea. Squared multiple correlation ranged from 0.733 to 0.916 and 0.699 to 0.901 in the U.S and South Korea, respectively. The results of intention to adopt anti-spyware programs are showed in Table 4-18.

Table 4-18. Factor Loading and Squared Multiple Correlation of Intention to Adopt Anti-Spyware Programs

Item	U.S		South Korea	
	Factor Loading	SMC	Factor Loading	SMC
Prediction of Use (IA2)	.889	0.790	.920	0.847
Intention to Use (IA3)	.957	0.916	.949	0.901
Recommending to Others (IS4)	.856	0.733	.836	0.699

Table 4-19. Scale Refinement of Intention to Adopt Anti-Spyware Programs

Nation	Items	# items	df	χ^2	p	χ^2/df	RMSEA	GFI	AGFI	CFI
U.S	IA1…IA5	5	5	45.340	0.000	9.068	0.151	0.952	0.856	0.978
	IA2…IA4*	3	0							
South Korea	IA1…IA5	5	5	53.110	0.000	10.622	0.171	0.939	0.817	0.969
	IA2…IA4*	3	0							

(1) IA1 had high error correlations with IA2 (U.S.: 9.905, South Korea: 5.613) and IA4 (South Korea: 12.294). Thus IA1 was dropped for parsimony.

(2) MI indicated high error correlation between IA4 and IA5 (U.S.: 25.309, South Korea: 17.292). IA5 also had low factor loading in South Korea (0.552), and thus it was dropped.

(3) Statistical fit cannot be obtained from only three items (0 of degree of freedom)

(7) Internal Consistency

The internal consistency of each construct was measured by examining estimates of composite reliability and variance extracted (Hair et al. 1998). Composite reliability refers to the extent to which the construct is represented by the indicators. It is computed conformance with the formula described by Werts et al. (1974). Compared to Cronbach's alpha, which provides a lower bound estimate of the internal consistency, the composite reliability is a more rigorous estimate for the reliability (Chin & Gopal, 1995). The overall amount of variance in the indicators accounted for by the variable reflects the extent to which the indicators are truly representative of the construct (Bassellier et al, 2003).

The recommended values of composite reliability for acceptable model reliability are above 0.70 (Werts, Linn, & Jöreskog, 1974; Gefen, Straub, & Boudreau, 2000) and for strong reliability are above 0.80 (Koufteros, 1999). All results in the U.S. and South Korea, as presented in Table 4-20, exceeded or converged the recommended value of 0.7 for composite reliability and of 0.5 for variance explained (Hair et al. 1998).

Table 4-20. Reliability and Variance Extracted

Variable	# items	U.S		South Korea	
		Reliability	Variance Extracted	Reliability	Variance Extracted
Computer Familiarity	5	0.832	0.498	0.857	0.546
Internet Familiarity	3	0.942	0.844	0.803	0.577
Security Familiarity	5	0.942	0.763	0.949	0.787
Knowledge of Spyware	4	0.826	0.544	0.833	0.558
Perceived Risk of Spyware	4	0.886	0.662	0.859	0.604
Trust of Anti-Spyware Programs	4	0.887	0.664	0.837	0.562
Intention to Adopt Anti-Spyware Programs	3	0.847	0.650	0.857	0.667

(8) Discriminant Validity

Discriminant validity refers to the extent to which the measures for each construct are distinctively different from each other. It is generally assessed by testing whether the correlations between pairs of dimensions are significantly different from unity (Anderson & Gerbing, 1998). Following Fornell and Lacker (1981), discriminant validity was tested. Because the squared correlations between constructs were lower than variance extracted, constructs are distinct. The results are presented in Table 4-21 and 4-22.

Table 4-21. Correlations and Discriminant Validity in the U.S.

	CF	IF	SF	KS	PRS	TA	IA
Computer Familiarity	0.498*						
Internet Familiarity	0.368	0.844*					
Security Familiarity	0.735	0.424	0.763*				
Knowledge of Spyware	0.763	0.246	0.752	0.544*			
Perceived Risk of Spyware	0.387	0.304	0.383	0.481	0.662*		
Trust of Anti-Spyware Programs	0.432	0.314	0.355	0.476	0.510	0.664*	
Intention to Adopt Anti-Spyware Programs	0.518	0.317	0.444	0.600	0.564	0.622	0.650*

* Variance extracted; others correlation coefficient

Table 4-22. Correlations and Discriminant Validity in South Korea

	CF	IF	SF	KS	PRS	TA	IA
Computer Familiarity	0.546*						
Internet Familiarity	0.245	0.577*					
Security Familiarity	0.592	0.259	0.787*				
Knowledge of Spyware	0.653	0.085	0.579	0.558*			
Perceived Risk of Spyware	0.352	0.327	0.312	0.424	0.604*		
Trust of Anti-Spyware Programs	0.294	0.209	0.299	0.347	0.316	0.562*	
Intention to Adopt Anti-Spyware Programs	0.303	0.224	0.290	0.382	0.376	0.630	0.667*

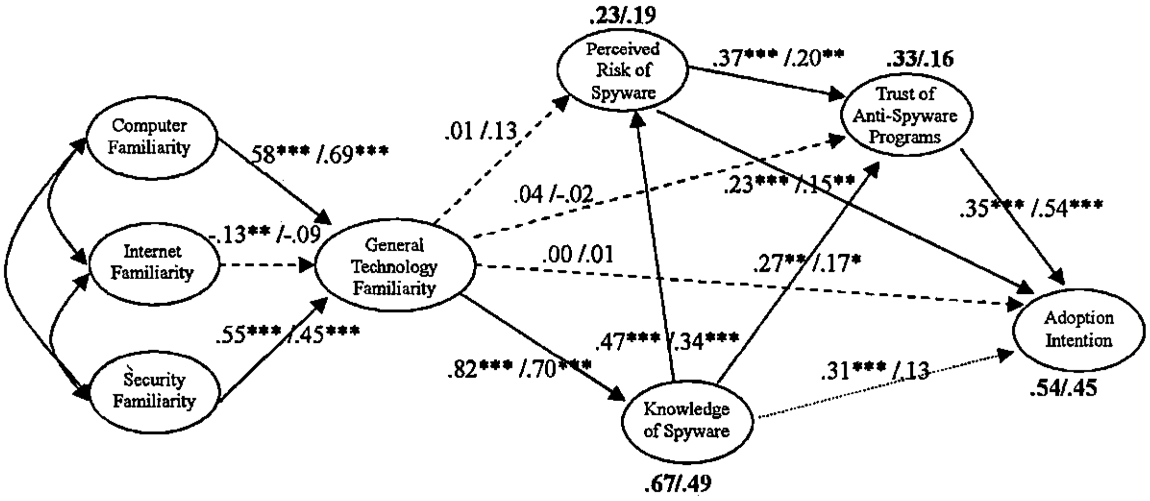
* Variance extracted; others correlation coefficient

4. Structural Model

Using a revised measurement model, structural equation modeling (SEM) was conducted to test the hypothesized relationships. This study hypothesized that technology familiarity, knowledge of spyware, perceived risk of spyware, and trust of anti-spyware programs directly impact intention to adopt anti-spyware programs.

(1) Initial Model

Figure 4-1. Initial Structural Model



U.S./South Korea, Bold means variance explained

* p <.05, **p<0.01, ***p <.001

———▶ Significant in Both

- - - - - - - ▶ Non-Significant in Both

·············▶ Significant in One

The model in Figure 4-1 explained 54% of U.S. respondents and 45% of South Korean respondents' intention to adopt anti-spyware programs. Although general technology familiarity was not a direct indicator of anti-spyware adoption intention, this was a meaningful result because this study was designed to find factors which maximize the explanation in the variance of the dependent variable.

Knowledge of spyware was also explained by 67% of U.S. respondents and 49% in South Korean respondents by general technology familiarity, as well. Although significance resulted, Internet familiarity was not supported in the U.S. because of the resulting negative relationship instead of the suggested positive relationship. Internet familiarity was not significant in South Korea. On the other hand, computer familiarity and security familiarity were significant dimensions of general technology familiarity in the U.S. and South Korea. Hypotheses related to technology familiarity were not significant at the $p<0.05$ level except H1 (General Technology Familiarity → Knowledge of Spyware) in U.S and South Korea.

Other hypotheses were significant in the U.S. and South Korea except H7 (Knowledge of Spyware → Intention to Adopt Anti-Spyware Programs) in South Korea. Table 4-23 presents the standardized path coefficients and statistical significance of the structural model in U.S and South Korea.

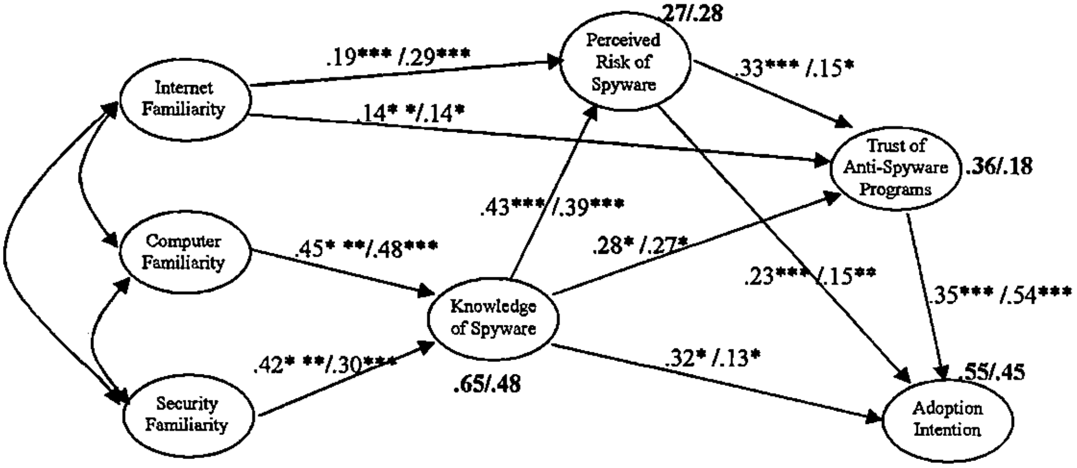
Table 4-23. Standardized Path Coefficients and Significances of Initial Model

Path		U.S (N=357)		South Korea (N=326)	
		Standardized Path Coefficient	Statistical Significance	Standardized Path Coefficient	Statistical Significance
Computer Familiarity → General Technology Familiarity		0.576	***	0.689	***
Internet Familiarity → General Technology Familiarity		-0.127	.009**	-0.091	.166
Security Familiarity → General Technology Familiarity		0.548	***	0.449	***
H1	General Technology Familiarity → Knowledge of Spyware	0.817	***	0.701	***
H2	General Technology Familiarity → Perceived Risk of Spyware	0.011	.907	0.131	.131
H3	General Technology Familiarity → Trust of Anti-Spyware Programs	0.042	.629	0.118	.107
H4	General Technology Familiarity → Intention to Adopt Anti-Spyware Programs	0.009	.897	0.007	.921
H5	Knowledge of Spyware → Perceived Risk of Spyware	0.472	***	0.341	***
H6	Knowledge of Spyware → Trust of Anti-Spyware Programs	0.266	**.004****	0.172	**.041***
H7	Knowledge of Spyware → Intention to Adopt Anti-Spyware Programs	0.314	***	0.127	.070
H8	Perceived Risk of Spyware → Trust of Anti-Spyware Programs	0.365	***	0.197	**.002****
H9	Perceived Risk of Spyware → Intention to Adopt Anti-Spyware Programs	0.230	***	0.150	**.004****
H10	Trust of Anti-Spyware Programs → Intention to Adopt Anti-Spyware Programs	0.351	***	0.537	***

* p <.05, **p<0.01, ***p <.001

(2) Revised Model

Figure 4-2. Revised Structural Model



U.S./South Korea, Bold means variance explained

* p <.05, **p<0.01, ***p <.001

———► Significant in Both

This study used reflective indicators and formative dimensions (Petter et al. 2007) to measure multidimensional general technology familiarity. Although Internet familiarity had a positive correlation with computer familiarity and security familiarity, Internet familiarity was a significantly negative dimension in the U.S.; and it was not significant in South Korea. Also, general technology familiarity only significantly influences knowledge of spyware (H1). The modification index showed that Internet Familiarity → Perceived Risk of Spyware (MI: 13.533) and Internet Familiarity → Trust of Anti-Spyware Programs (MI: 6.916) in the U.S. and Internet Familiarity → Perceived Risk of Spyware (MI: 23.619) in South Korea, which exceeded 3.84 of MI, suggesting that adding that path may significantly improve model fit (Hair et al. 1998). Thus, this study presented a second structural model. Because technology familiarity was not significant for H2 (General Technology Familiarity → Perceived Risk of Spyware), H3 (General Technology Familiarity → Trust of Anti-Spyware Programs), and H4 (General Technology Familiarity → Intention to Adopt Anti-Spyware Programs) in the initial structural model, the revised structural model no longer incorporated the formative dimension for multidimensional technology familiarity. Based on modification index, this study separately examined the relationships for computer familiarity, Internet familiarity, and security familiarity. Thus, this analysis yielded four new hypotheses:

NH1: Internet familiarity is positively related to perceived risk of spyware.

NH2: Internet familiarity is positively related to trust of anti-spyware programs.

NH3: Computer familiarity is positively related to knowledge of spyware.

NH4: Security familiarity is positively related to knowledge of spyware.

In the revised structural model, all ten hypotheses, including the four new hypotheses, were significant at the $p < 0.05$ level in the U.S. and South Korea. Standardized path coefficients and significances of revised model were presented in Table 4-24.

Table 4-24. Standardized Path Coefficients and Significances of Revised Model

Path		U.S (N=357)		South Korea (N=326)	
		Standardized Path Coefficient	Statistical Significance	Standardized Path Coefficient	Statistical Significance
NH 1	Internet Familiarity → Perceived Risk of Spyware	0.192	***	0.288	***
NH 2	Internet Familiarity → Trust of Anti-Spyware Programs	0.141	**0.007****	0.139	**.026***
NH 3	Computer Familiarity → Knowledge of Spyware	0.453	***	0.477	***
NH 4	Security Familiarity → Knowledge of Spyware	0.415	***	0.298	***
H5	Knowledge of Spyware → Perceived Risk of Spyware	0.427	***	0.393	***
H6	Knowledge of Spyware → Trust of Anti-Spyware Programs	0.278	***	0.27	***
H7	Knowledge of Spyware → Intention to Adopt Anti-Spyware Programs	0.321	***	0.131	**.015***
H8	Perceived Risk of Spyware → Trust of Anti-Spyware Programs	0.332	***	0.154	**.021***
H9	Perceived Risk of Spyware → Intention to Adopt Anti-Spyware Programs	0.230	***	0.152	**.004****
H10	Trust of Anti-Spyware Programs → Intention to Adopt Anti-Spyware Programs	0.351	***	0.537	***

* p <.05, **p<0.01, ***p <.001

(3) Model Fit of Structural Model

The initial model fit was compared to the revised model fit. The initial model and the revised model both had acceptable indexes of Adjusted Goodness of Fit Index (AGFI), Root Mean Square Error of Approximation (RMSEA), Normed Fit Index (NFI), Non-Normed Fit Index (NNFI) and Comparative Fit Index (CFI). Overall, in the revised model, the fit was slightly increased. Thus, this study adopted the revised model to describe anti-spyware program adoption. Goodness of Fit indices was presented in Table 4-25.

Table 4-25. Goodness-of Fit indices for the Initial and Revised Structural Model

	Initial Model		Revised Model		Desired Level
	U.S	South Korea	U.S	South Korea	
χ^2	682.730	850.266	668.525	826.784	Smaller
df	335	335	337	337	-
χ^2/df	**2.038**	**2.538**	**1.984**	**2.453**	<3.0
GFI	0.881	0.836	0.884	0.842	>0.9
AGFI	**0.856**	**0.802**	**0.860**	**0.810**	>0.8
RMR	0.096	0.115	0.087	0.096	<0.05
RMSEA	**0.054**	**0.068**	**0.053**	**0.067**	<0.08
NFI	**0.940**	**0.906**	**0.941**	**0.908**	>0.90
NNFI	**0.964**	**0.933**	**0.966**	**0.936**	>0.90
CFI	**0.968**	**0.940**	**0.970**	**0.943**	>0.90

Table 4-26 and Table 4-27 display the results of hypothesis testing of initial and revised structural model.

Table 4-26. Results of Hypothesis Testing of Initial Structural Model

Num	Hypothesis	U.S.	South Korea
H1	General technology familiarity is positively related to the knowledge of spyware.	Supported	Supported
H2	General technology familiarity is positively related to perceived risk of spyware.	Not Supported	Not Supported
H3	General technology familiarity is positively related to trust of anti-spyware programs.	Not Supported	Not Supported
H4	General technology familiarity is positively related to adoption intention.	Not Supported	Not Supported
H5	Knowledge of spyware is positively related to perceived risk of spyware.	Supported	Supported
H6	Knowledge of spyware is positively related to trust of anti-spyware programs.	Supported	Supported
H7	Knowledge of spyware is positively related to adoption intention.	Supported	Not Supported
H8	Perceived risk of spyware is positively related to trust of anti-spyware programs.	Supported	Supported
H9	Perceived risk of spyware is positively related to adoption intention.	Supported	Supported
H10	Trust of anti-spyware programs is positively related to adoption intention.	Supported	Supported
H11	Significant differences exist in anti-spyware adoption attitude between the U.S. and South Korea.	Supported	

Table 4-27. Results of Hypothesis Testing of Revised Structural Model

Num	Hypothesis	U.S.	South Korea
NH1	Internet familiarity is positively related to perceived risk of spyware.	Supported	Supported
NH2	Internet familiarity is positively related to trust of anti-spyware programs.	Supported	Supported
NH3	Computer familiarity is positively related to knowledge of spyware	Supported	Supported
NH4	Security familiarity is positively related to knowledge of spyware	Supported	Supported
H5	Knowledge of spyware is positively related to perceived risk of spyware.	Supported	Supported
H6	Knowledge of spyware is positively related to trust of anti-spyware programs.	Supported	Supported
H7	Knowledge of spyware is positively related to adoption intention.	Supported	Supported
H8	Perceived risk of spyware is positively related to trust of anti-spyware programs.	Supported	Supported
H9	Perceived risk of spyware is positively related to adoption intention.	Supported	Supported
H10	Trust of anti-spyware programs is positively related to adoption intention.	Supported	Supported
H11	Significant differences exist in anti-spyware adoption attitude between the U.S. and South Korea.	Supported	

In chapter 5, this study presents discussion of the results, implications, limitations, and conclusions of the study.

Chapter 5
Discussion and Conclusion

Chapter 5 presents a discussion of the results, implications for researchers, business practitioners, and educators, limitations, and conclusions of the study.

1. Discussion of Results

In this study, several constructs were adopted and modified from previous studies, and then, statistical methods (exploratory factor analysis, confirmatory factor analysis, and structural equation modeling) were used to examine the impact of the variables in anti-spyware program adoption. The hypothesized model was developed to explain the relationship between constructs. In the following section, the results are discussed.

General Technology Familiarity

In the initial structural model, general technology familiarity was only positively significant to knowledge of spyware. (U.S: β[6] $= 0.817$, $p<0.001$, South Korea: $\beta = 0.701$, $p<0.001$) while not significant to perceived risk of spyware (U.S: $\beta = 0.011$, $p=0.907$, South Korea: $\beta = 0.131$, $p=0.131$), trust of anti-spyware programs (U.S:

[6] β represents a standardized path coefficient, which is used to examine the causal relationship between constructs. β can be compared to assess the relative effects of the constructs within the structural model. The higher value means the higher effect size.

β = 0.042, p=0.629, South Korea: β = 0.118, p=0.107), and intention to adopt anti-spyware programs (U.S: β = 0.009, p=0.897, South Korea: β = 0.007, p=0.921). This study suggests that general technology familiarity is so general that it cannot directly affect behavior intention, meaning that a mediator (e.g. knowledge) is needed to affect behavior intention.

This study used the formative construct (computer, Internet, security familiarity) to examine multiple dimensions of general technology familiarity. Contrary to the expectation, internet familiarity (U.S: β = -0.127, p=0.009, South Korea: β = -0.091, p=0.166) was not positively significant dimension of general knowledge familiarity. In the same vein, compared with computer and security familiarity, the mean of Internet familiarity was high. It can be explained, in general cases, that computer users are highly familiar with Internet, so that Internet familiarity cannot be examined with computer and security familiarity in general technology familiarity. In the meantime, the modification index indicated that Internet familiarity positively influences perceived risk of spyware and trust of anti-spyware programs. Therefore, this study separately examined computer, Internet and security familiarity, not in one construct, and then tested the revised structural model. The following is the results and discussions of the revised structural model

New Hypothesis 1: Internet familiarity is positively related to perceived risk of spyware.

New Hypothesis 2: Internet Familiarity is positively related to trust of anti-spyware programs.

Internet familiarity was found to have a positive influence on the perceived risk of spyware (U.S: β = 0.192, p<0.001, South Korea: β = 0.288, p<0.001) and trust of anti-spyware programs (U.S: β = 0.141, p=0.007, South Korea: β = 0.139, p=0.026). Unlike computer and security familiarity, Internet familiarity did not significantly influence knowledge of spyware. A possible explanation is that individuals could access spyware and anti-spyware programs through Internet usage. They possibly perceive risk of spyware and trust of anti-spyware programs without knowledge of spyware.

This study concludes that general knowledge of the Internet influences negative belief of spyware and positive belief of anti-spyware programs, supporting the argument that knowledge influence belief (Jasperson, et al. 2003).

New Hypothesis 3: Computer familiarity is positively related to the knowledge of spyware.

New Hypothesis 4: Security familiarity is positively related to the Knowledge of Spyware.

Computer familiarity (U.S: β = 0.453, p<0.001, South Korea: β = 0.477, p<0.001) and Security Familiarity (U.S: β = 0.415, p<0.001, South Korea: β = 0.298, p<0.001) were found to be a significant and positive predictor of the knowledge of spyware in both the U.S. and South Korea. Also, a large part of the variance in knowledge of spyware (U.S: 65%, South Korea: 48%) was explained by computer familiarity and security familiarity. The results indicate that relatively general knowledge (computer and security) is an important determinant of specific knowledge (spyware).

Hypothesis 5: Knowledge of spyware is positively related to perceived risk of spyware

Hypothesis 6: Knowledge of spyware is positively related to trust of anti-spyware programs

Hypothesis 7: Knowledge of spyware is positively related to adoption intention.

Knowledge of spyware was found to be a significant and positive predictor of perceived risk of spyware (U.S.: β =0.427, $p<0.001$, South Korea: β =0.393, $p<0.001$), trust of anti-Spyware programs (U.S.: β =0.278, $p<0.001$, South Korea: β =0.270, $p<0.001$), and intention to adopt anti-spyware programs (U.S.: β =0.321, $p<0.001$, South Korea: β =0.131, $p=0.015$).

These results support the Dinev and Hu's finding that the key predictor of protective technology adoption (anti-spyware programs) is awareness of negative technology (spyware). Also, this study supports that knowledge is a determinant of intent to act (Gefen at al. 2003, Roger, 1995). This study shows that knowledge of negative technology influences two beliefs: perceived risk of negative technology and trust of protective technology, helping to confirm that knowledge is a predictor of belief (Jasperson et al. 2003).

Also, this study addresses the relationship between knowledge behavior intention in the initial and revised structural models. In the initial structural model, knowledge to behavior intention was positively significant in the U.S. (β =0.314, p<0.001), but not in South Korea (β =0.127, p=0.070). The possible explanation is type I error, occurring when a researcher believes there is a genuine effect in the population when in fact there isn't. In the revised model, knowledge to behavior intention show relatively high different effect size, while knowledge to perceived risk and trust show similar effect sizes in the U.S. and South Korea. Knowledge could be an important predictor of behavior intention in the U.S.

Hypothesis 8: Perceived risk of spyware is positively related to trust of anti-spyware programs

Hypothesis 9: Perceived risk of spyware is positively related to adoption intention.

Perceived risk of spyware was found to be a significant and positive predictor of trust of anti-spyware programs (U.S.: β =0.332, p<0.001, South Korea: β =0.154, p=0.021) and intention to adopt anti-spyware programs (U.S.: β =0.230, p<0.001, South Korea: β =0.152, p=0.004). H8 supports the saying that "the enemy of my enemy is my friend". H9 supports the role of risk as a predictor of intention to adopt protective technology.

Hypothesis 10: Trust of anti-spyware programs is positively related to adoption intention

Trust of anti-spyware programs was found to be a significant and positive predictor of intention to adopt anti-spyware programs (U.S.: β =0.351, p<0.001, South Korea: β =0.537, p<0.001). H10 supports that trust is a predictor of intention to act (Bhattacherjee, 2002; Gefen et al, 2003).

Hypothesis 11: Significant differences exist in anti-spyware adoption attitude between the U.S. and South Korea.

Regarding all constructs, the U.S. results were significant stronger than South Korea at the 0.05 level. Possible explanations regarding Korean's low consciousness of security are discussed next.

Compared to the rate of high speed internet penetration, Koreans' security consciousness is very low (Kim, 2004). Korean Internet users recognize the issue of personal information privacy and know how to prevent their privacy, but they do not intend to act to prevent the danger (Kil, 2008). This phenomenon is reflected by the low rate of anti-virus program usage in South Korea. Compared with the U.S. (71%) and Japan (74%), the rate of anti-virus program usage in Korea is 38% (Kim, 2004).

The results of the current study showed that 66.9% U.S. respondents used anti-spyware programs while 52.6% Korean respondents used anti-spyware programs. Some researchers presented cultural aspects regarding Koreans' low security and privacy concerns. According to Sung (2004), Koreans have been in a unified community with large family systems and have had rare chances at privacy. For example, although somebody opens another person's private mail, he or she does not realize that it is a severe privacy infringement.

2. *Implications*

The findings of this study contribute to the body of work on protective technology adoption for practitioners, researchers, and educators.

For practitioners, the findings of this study will help online firms and anti-spyware sites. Online firms will be able to provide solutions to protect consumers from negative technologies such as viruses and spyware, therefore reliving users' concern. This, in turn, will enhance consumers' trust in Web sites. Furthermore, anti-spyware sites can more effectively develop their Web sites by providing users with online education in local and global aspects.

This study determined the predictors of anti-spyware program adoption. In the context of protective technology adoption, Dinev and Hu (2007) argued that conventional motivational factors such as perceived usefulness and perceived ease of use become less meaningful or at least less significant. Also, awareness of negative technology is an important predictor of intention to adopt protective technology. This study extended the anti-spyware adoption research of previous studies. This study also found that computer and security familiarity are important predictors of knowledge of spyware.

The extended theory of user behavior presented in this study is not bound to protective technology adoption. Knowledge of technologies or knowledge of problems and the ways to solve the problems will be significant to a wide range of innovation at individual, organizational, and interorganizational level (Dinev & Hu, 2007). This study also contributes to individual's knowledge and behavior toward spyware.

This study identified the relationships between familiarity and knowledge. Although computer and security familiarity are important predictors of knowledge of spyware, they do not significantly influence protective technology adoption. This study assumes that the familiarity is too general to influence intention to act. In order to influence user behavior, relatively specific knowledge is required.

This study also found that the research model adopted in the U.S can be used in South Korea.

Finally, the findings also contribute to knowledge and security education. Based on the findings of this study, educators can teach general information which influence specific knowledge. Also, this study will help educators design relevant security information systems courses.

3. Limitations

This study has several limitations. First, this study used a student sample in the U.S. and South Korea. However, students can be used effectively as surrogates in the context of technology adoption (McKnight et al. 2002).

Second, using a convenience sample is a limitation in terms of the representativeness of the population. This study was based on a convenience sample which lacks empirical representativeness to the larger technology user population.

Third, this study used only one university in each country. In addition to cross cultural differences, the two universities have difference backgrounds (e.g. public vs. private and rural vs. suburban). Possible biases from these factors, which this study did not consider, could exist.

Fourth, sample bias could exist in the study. The South Korean sample includes 19.1 % engineering majors which are assumed as being highly familiar with computer and Internet.

Fifth, although this study followed the guideline of cross-cultural research (Karahanna et al. 2002), administrative error in translation and survey administration may have occurred. Karahanna et al. (2002) suggested that "to translate correctly, there is a need to translate to the target language - which needs to be performed by a native speaker of the target language-and then back translate to the original language, this time by a different native speaker of the original language". While the first translation to Korean was conducted by a native Korean, translation back to the English by a native was not conducted. Thus, this process may have produced possible error in the cross cultural research.

4. Future Research

Many opportunities exist for future research related to this study. For example, future research could explore other variables which influence protective technology adoption. Future research could also examine the relationship of demographic variables (e.g. gender, age, and major) to protective technology adoption. The current study identified two groups (the U.S. and South Korea); other comparison groups could be studied in the future. Also, different subjective norms in the U.S. and South Korea could be examined.

Further research could also identify how broad knowledge influences specific knowledge. While the research model can be adopted in both the U.S. and South Korea, this study found significant differences. Cultural aspects could be explored as a determinant of the differences in global IS research.

4. Conclusion

Although numerous studies on technology adoption have been conducted, research on negative technology and protective technology adoption has been limited in information systems research (Dinev & Hu, 2007). Also, cross-cultural IS research has been less developed (Karahanna et al. 2002). This study started with the need to combine between protective technology adoption and cross-cultural research between countries. Comparing the U.S. with South Korea, this study examined factors of anti-spyware adoption and extended the work of previous research.

This study found that knowledge, perceived risk and trust are important predictors of protective technology adoption. Also computer and security familiarity are important predictors of knowledge of negative technology such as spyware.

In sum, this study built upon previous research to contribute to technology adoption and cross cultural research in information systems.

References

Agarwal, R., & Karahanna, E. (2000). Time flies when you're having fun: cognitive absorption and beliefs about information technology usage. *MIS Quarterly*, 24(4), 665-694

Agarwal, R., & Prasad, J. (1998). A conceptual and operational definition of personal innovativeness in the domain of information technology. *Information Systems Research*, 9(2), 204–215.

Ajzen, I. (1988). *Attitudes, Personality, and Behavior*, The Dorsey Press, Chicago, IL.

Alba, J. W., & Hutchinson, J. W. (1987). Dimensions of consumer expertise. *Journal of Consumer Research*, 13(4), 411-454.

Anckar, B. (2003). Consumer intentions in terms of electronic travel distribution. *e-Service Journal*, 2(2). 68-86.

Anderson, J. C., and Gerbing, S. W. (1998). Structural equation modeling in practice: a review and recommended two step approach. *Psychological Bulletin*, 103(3), 411-423.

Asaravala, A. (2004, March). Prepare for adware. *Wired News*. Retrieved Oct 28, 2008, from www.wired.com/news/print/0,1294,63345,00.html.

Awad, N. F., & Fitzgerald, K. (2005). The deceptive behaviors that offend us most about spyware. *Communication of the ACM*, 48, 55-60.

Babbie, E. (1995). *The Practice of Social Research*. Belmont, CA: Wadsworth Publishing Company.

Bagozzi, R. P., & Fornell, C. (1982). Theoretical concepts, measurement, and meaning. C.Fornell, ed. A Second Generation of Multivariate Analysis, Vol. 2. Praeger, New York, 5-23.

Baker, W. M. (2006). What's your main technology concern? *Strategic Finance*, December, 49-54.

Bassellier, G., Benbasat, I., & Reich, B. H., (2003). The influence of business managers' IT competence on championing IT. *Information Systems Research*, 14(4), 317-336.

Beith, M. (2005), Spyware vs. anti-spyware. *Newsweek.* Jan(1), 30.

Bhattacherjee, A. (2002). Individual trust in online firms: scale development and initial test. *Journal of Management Information Systems,* 19(1), 211-241.

Biswas, A. (1992). The moderating role of brand familiarity in reference price perceptions. *Journal of Business Research,* 15{3), 251-262.

Bruner, G. C., & Kumar, A. (2000). Web commercials and advertising hierarchy-of-effects. *Journal of Advertising Research,* 40(1/2), 35-43.

Byrne, B. M. (2001). *Structural Equation Modeling with AMOS: Basic Concepts, Applications, and Programming.* Mahwah, NJ: Lawrence Erlbaum Associates.

Chin, W., & Gopal, A. (1995). Adoption intention in GSS: importance of beliefs, *Data Base Adv,* 26, 42-64.

Churchman, C. W. (1971). *The Design of Inquiring Systems: Basic Concepts of Systems and Organization.* Basic books, Inc., New York.

Clyman, J. (2004). Antispyware. *PC Magazine,* 23(13), 89.

Cohen, J. E. (2003). DRM and privacy. *Communications of the ACM,* 46(4), 46-49.

Consumer Reports. (2008). Protect yourself online, 73(9), 23-25.

Dambrot, F. H., Watkins-Malek, M. A., Silling, M. S., Marshall, R. S., & Garver, J. A. (1985). Correlates of sex differences in attitudes toward involvement with computers. *Journal of Vocational Behavior,* 27, 71-86.

Daniels, J. (2004). Scumware.biz educates about dangers of adware/scumware. *Computer Security Update,* 5(2), 7-9.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use and user acceptance of information technology. *MIS Quarterly,* 13(3), 319-340.

Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989). User acceptance of computer technology: a comparison of two theoretical models. *Management Science,* 35(8), 982-1003.

Delbridge, A., Bernard, J. R. L. (1998). *The Concise Macquarie English Dictionary* (3rd ed). Sydney: Macquarie University.

Dinev, T., & Hu, Q. (2007). The centrality of awareness in the formation of user behavioral intention toward protective information technology. *Journal of the Association for Information Systems,* 8(7). 386-408.

Downey, R. G., & King, C. V. (1998). Missing data in Likert ratings: a comparison of replacement methods – method for measuring attitudes developed by R. Likert. *Journal of General Psychology*, 125(2), 175-191.

Economist. (2004). A hidden menace. June (5), 61-66.

Edwards, J. (2004). Senator Edwards Proposes Spyware Law. Retrieved July 29, 2004, from http://www.senate.gov/~edwards /press/2000/oct05-pr.html.

Fishbein, M., & Ajzen, I. (1975). *Belief, Attitude, Intention and Behavior: An Introduction to Theory and Research*. Addison-Wesley, Reading, MA.

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research*, 18(1), 39-50.

Freeman, L. A., & Urbaczewski, A. (2005). Why do people hate spyware? *Communication of the ACM*, 48, 50-53.

Gefen, D. (2000). E-commerce: the role of familiarity and trust. *Omega*, 28(5), 725-737.

Gefen, D., Karahanna, E., and Straub, D. W. (2003). Trust and TAM in online shopping: an integrated model. *MIS Quarterly* 27(1), 51-90.

Gefen, D., Straub, D. W., & Boudreau, M. C. (2000). Structural equation modeling and regression: guidelines for research practice. *Communications of AIS*, 4(7), 1-79.

Gibson, S. (2005). Spyware was inevitable. *Communication of the ACM*, 48, 37-39.

Ha, H., & Perks, H. (2005). Effects of consumer perceptions of brand experience on the web: brand familiarity, satisfaction and brand trust. *Journal of Consumer Behavior*, 4(6), 438-452.

Hair, J. F., Tatham, R. L.,. Anderson, R. E., & Black, W. (1998). *Multivariate Data Analysis*. New York: Pearson Education.

Hart, P., & Saunders, C. (1997). Power and trust: critical factors in the adoption and use of electronic data interchange. *Organization Science*, 8(1), 23-42.

Hoch, S. J., & Deighton, J. (1989). Managing what consumers learn from experience. *Journal of Marketing*, 53, 1-20.

Hofstede, G. (1980). *Culture's Consequences: International Differences in Work-Related Values*, Sage Publications, Beverly Hills, CA.

Hofstede, G. (1993). Cultural constraints in management theories. *Academy of Management Executive*, 7(1), 81-105.

Hwang, W., Jung, J., & Salvendy, G. (2006). Internationlisation of e-commerce: a comparison of online shopping preferences among Korean, Turkish and U.S. populations. *Behaviour & Information Technology*, 25(1), 3-18.

Jarvenpaa, S. I., Tractinsky, N., & Vitale, M. (2000). Consumer trust in an Internet store. *Information Technology andManagement*. 1(2), 45-71.

Jarvenpaa, S. L., & Tractinsky, N. (1999). Consumer trust in an Internet store: a cross-cultural validation. *Journal of Computer-Mediated Communication*. 5, 1-35.

Jasperson, J. L., Zmud, R. W., & Sambamurthy, V. (2003). The role of individuals' knowledge in explanations about the postadoptive use of enterprise IT applications. Working paper, Michael Price College of Business, University of Oklahoma, Norman, OK.

Karahanna, E., Evaristo, R., & Strite, M. (2002), Methodological issues in MIS cross-cultural research. *Journal of Global Information Management*, 10(1), 48-55.

Karahanna, E., Evaristo, R., & Strite, M. (2005), Level of culture and individual behavior: an integrative perspective. *Journal of Global Information Management*, 13(2), 1-20.

Karahanna, E., Straub, N. L., & Chervany, N. L. (1999). Information technology adoption across time: a cross-sectional comparison of pre-adoption and post-adoption beliefs. *MIS Quarterly*, 23(2), 183-213.

Karvonen, K., Cardholm, L., & Karlsson, S. (2000). Cultures of trust: a cross-cultural study on the formation of trust in an electronic environment, The Fifth Nordic Workshop on Secure IT Systems, 12-13 Oct. Retrieved October 12, 2008, from the www.tml.tkk.fi/Research/TeSSA/Papers/Karvonen/Karvonen_Cardholm_Nor dsec_final.pdf

Kenyon, H.S. (2004). Spyware stymies network operators. *Armed Forces Communications and Electronics Association,* 58(12), 47–48.

Kil, M (2008, January, 17). Low security consciousness of individual PC users, *Boannews*, Retrieved December 20, 2008, from the http://www.boannews.com/media/view.asp?idx=8650&kind=1

Kim, K. (2004, July 29). Korea where hackers go through. *Josunilbo,* Retrieved December 20, 2008, from the http://weekly.chosun.com/site/data/html dir /2004/07/28/2004072877024.html

Kline, R. B. (2005). *Principles and practice of structural equation modeling.* 2nd ed. New York: Guildford.

Komiak, S. Y. X., & Benbasat, I. (2006). The effects of personalization and familiarity on trust and adoption of recommendation agents. *MIS Quarterly,* 30(4), 941-960.

Koufteros, X. A. (1999). Testing a model of full production: a paradigm for manufacturing research using structural equation modeling. *Journal of Operations Management,* 17, 467-488.

LaRose, R., Rifon, N. J., & Enbody, R. (2008). Promoting personal responsibility for Internet safety. *Communications of the ACM,* 51(3), 71-76.

Lee, Y., & Kozar, K. A. (2005). Investigating factors affecting the adoption of anti-spyware systems. *Communication of the ACM,* 48, 72-77.

Lee, Y., & Kozar, K. A. (2008). An empirical investigation of anti-spyware software adoption: a multitheoretical perspective. *Information & Management,* 45(2), 109-119.

Luftman, J., & McLean, E. R. (2004). Key issues for IT executives. *MIS Quarterly Executive,* 3(2), 89-104.

Luhmann, N. (1979). Trust and Power, John Wiley & Sons, Chichester, England.

Mason, R. O. (1986). Four ethical issues of the information age. *MIS Quarterly,* 10(4), 4-12.

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. *Academy of Management Review* (20)3, 709-734.

McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and validating trust measures for e-commerce: an integrative typology. *Information Systems Research*. 13(3), 334-359.

Merchant, R., & Sullivan, C. (1983). Microcomputers for everyone. *Community College Review*, 10, 8-11.

Nelson, L. J., Wiese, G M., & Cooper, J. (1991). Getting started with computers: experience, anxiety, and relational style. *Computers in Human Behavior*, 7, 185-202.

Park, C., & Jun, J. (2002). A cross-cultural comparison of online buying intention: effects of Internet usage, perceived risks, and innovativeness. The 8th Australian World Wide Web Conference, 6-10 July, 472-84. Retrieved Oct 12, 2008, from www. ausweb.scu.edu.au/aw02/papers/refereed/park/paper.html

Petter, S., Straub, D., & Rai, A. (2007). Specifying formative constructs in information systems research. *MIS Quarterly*, 31(4), 623-656.

Poston, R., Stafford, T. F., & Hennington, A. (2005). Spyware: a view from the online street. *Communication of the ACM*, 48, 96-99.

Potosky, D., & Bobko, P. (1998). The computer understanding and experience scale: a self-report measure of computer experience. *Computers in Human Behavior*, 14(2), 337-348.

Rogers, E. M. (1995). *Diffusion of Innovations*, 4th ed. the Free Press, New York.

Rosen, L. D. & Sears, D. C., & Weil, M. M. (1987). Computerphobia. *Behavior Research Method, Instruments, and Computers*, 19, 167-179.

Schmidt, M. B., Johnston, A. C., Arnett, K. P., Chen, J. Q., & Li, S. (2008). A cross-cultural comparison of U.S. and Chinese computer security awareness. *Journal of Global Information Management*, 16(2), 91-103.

Schulenberg, S. E. & Melton, A. M. A. (2008). The computer aversion, attitude, and familiarity index (CAAFI): a validity study. *Computers in Human Behavior*, 24, 2620-2638.

Schulenberg, S. E., Yutrzenka, B. A., & Goham, C. L. (2006). The computer aversion, attitude, and familiarity index (CAAFI): a measure for the study of computer-related constructs. *Journal of Educational Computing Research*. 32(2), 129-146.

Security. (2008). Spyware legislation needed to curb increase in online security and privacy threats. July, 16.

Sheppard, B. H., Hartwick, J., & Warshaw, P. R. (1988). The theory of reasoned action: a meta analysis of past research with recommendations for modifications in future research. *Journal of Consumer Research*, 15 (3), 325-343.

Shukla, S. & Nah, F. (2005). Web browsing and spyware intrusion. *Communication of the ACM*, 48, 85-90.

Siala, H., O'Keefe, R. M., & Hone, K. S. (2004). The impact of religious affilation on trust in the context of electronic commerce. *Interacting with Computers*, 16, 7-27.

Van Slyke, C, Shim, J. T. Johnson, R. & Jiang, J. (2006). Concern for information privacy and online consumer purchasing. *Journal of the Association for Information Systems*, 7(6), 415-443.

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: measuring individuals' concerns about organizational practices. *MIS Quarterly*, 20(2), 167-196.

Spiros, G., Dimitriadis, S., & Stathakopoulos, V. (2005). Antecedents of perceived quality in the context of Internet retail stores. *Journal of Marketing Management*, 21, 669-700.

Spring, T. (2004). Striking back at spyware, *PC World*. 22(7), 36-38.

Stafford, T. F., & Urbaczewski, A. (2004). Spyware: the ghost in the machine. *Communications of the AIS*, 14, 291-306.

Steven, B., Gerald, L., & Eric, J. (1999). Predictors of online buying behavior, *Communications of the ACM*, 42, 32-38.

Straub, D., Loch, K., Evaristo, R., Karahanna, E., & Strite, M. (2002). Toward a theory-based measurement of culture. *Journal of Global Information Management*, 10(1), 13-23.

Strite, M., & Karahanna, E. (2006). The role of espoused national cultural values in technology acceptance, *MIS Quarterly*, 30(3), 679-704.

Sung, S. (2004). There is no cyber privacy(?) *Digital Contents*, April, 120-128.

Sveiby, K. E. (1997). *The new organizational wealth, managing and measuring knowledge-based assets.* Berret-koehler Publishers Inc., San Francisco, CA.

Taylor, S., & Todd, P. (1995). Understanding information technology usage: a test of competing models, *Information Systems Research*, 6(3), 144-176.

Triandis, H. C. (1989a). *Cross-Cultural Studies of Individualism and Collectivism* in Nebraska Symposium on Motivation, J. Berman (ed.), University of Nebraska Press, Lincoln, NE, 41-133

Venkatesh, V. (1999). Creation of favorable user perceptions: exploring the role of intrinsic motivation. *MIS Quarterly*, 23(2), 239–260.

Venkatesh, V. (2000). Determinants of perceived ease of use: integrating perceived behavioral control, computer anxiety and enjoyment into the technology acceptance model. Information *Systems Research*, 11 (4), 342–365.

Venkatesh, V., & Davis, F. D. (1996). A model of the antecedents of perceived ease of use: development and test. *Decision Sciences*, 27(3), 451-481.

Venkatesh, V., & Davis, F. D. (2000). A theoretical extension of the technology acceptance model: four longitudinal field studies. *Management Science*, 46(2), 186-204.

Venkatesh, V. & Morris, M. G. (2000). Why don't men ever stop to ask for directions? Gender, social influence and their role in technology acceptance and usage behavior. *MIS Quarterly*. Vol 24, 115-139.

Venkatesh, V., Morris, M. G., Davis, F. D., & Davis, G. B. (2003). User acceptance of information technology: toward a unified view. *MIS Quarterly*, 27, 425-478.

Warkentin M., Luo, X., & Templeton, G. F. (2005). A framework for spyware assessment. *Communications of the ACM*, 48(8), 79-84.

Wert, C. E., Linn, R. L., & Jöreskog, K. G (1974). Interclass reliability estimates: testing structural assumptions. *Education and Psychological Measurement*, 34, 25-33.

Whitman, M. E. (2003). Enemy at the gate: threat to information security. *Communications of the ACM, 46(8)*, 91-95.

Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: a threat control model and empirical test. *Computers in Human Behavior*, 24, 2799-2816.

Yi, M. Y., Jackson, J. D., Park, J. S., & Probst, J. C. (2006). Understanding information technology acceptance by individual professional: toward an integrative view. *Information and Management*, 43(3), 350-363.

Zhang, X. (2005). What do consumers really know about spyware? *Communication of the ACM*, 48, 45-48.

Appendixes

Appendix A. Descriptive statistics and ANCOVA for individual items

Code	Name	U.S.		South Korea		ANCOVA	
		Mean	S.D	Mean	S.D	F-value	P-value
CF1	Latest Hardware	3.50	1.645	3.64	1.425	.431	.512
CF2	Changing Hardware	3.90	1.865	3.00	1.681	64.437	.000***
CF3	Hardware Familiarity	4.06	1.747	3.23	1.640	61.219	.000***
CF4	Latest Software	3.77	1.691	3.64	1.569	3.484	.062
CF5	Changing Software	4.22	1.830	3.43	1.820	52.714	.000***
CF6	Software Familiarity	4.36	1.756	3.52	1.728	59.666	.000***
CF7	Reading Magazine	2.29	1.605	2.19	1.476	5.749	.017*
CF8	Computer Familiarity	4.85	1.613	3.76	1.552	93.621	.000***
Total Computer Familiarity		3.87	1.428	3.30	1.326	48.028	.000***
IF1	Search Engines	6.00	1.271	5.30	1.327	51.510	.000***
IF2	Email Use	6.44	0.896	5.38	1.278	157.447	.000***
IF3	Searching Information	6.45	0.845	5.72	1.122	93.077	.000***
IF4	Purchasing Products	5.80	1.440	5.42	1.371	11.469	.001***
IF5	Reading Articles	6.15	1.163	5.48	1.346	50.694	.000***
IF6	Internet Familiarity	6.49	0.863	5.64	1.145	115.942	.000***
Total Internet Familiarity		6.22	0.876	5.49	1.003	102.570	.000***
SF1	Privacy Violation	4.69	1.590	4.15	1.300	25.781	.000***
SF2	Protective Knowledge	4.49	1.595	3.50	1.259	86.676	.000***
SF3	Security Technology	4.26	1.646	3.29	1.241	89.228	.000***
SF4	Information Security	4.19	1.624	3.34	1.307	68.473	.000***
SF5	Computer Security	4.36	1.607	3.43	1.366	85.089	.000***
SF6	Internet Security	4.52	1.621	3.43	1.387	104.264	.000***
SF7	Security Familiarity	4.31	1.562	3.37	1.351	87.461	.000***
Total Security Familiarity		4.40	1.488	3.50	1.107	94.867	.000***
KS1	Updating Knowledge	3.24	1.687	2.76	1.499	24.477	.000***
KS2	Malicious Software	3.56	1.780	3.21	1.546	17.602	.000***
KS3	Seeking Advice	2.93	1.681	2.54	1.490	19.547	.000***
KS4	Problem & Results	3.50	1.832	2.74	1.481	53.361	.000***
KS5	Spyware Knowledge	3.36	1.723	2.80	1.406	37.919	.000***
Total Knowledge of Spyware		3.32	1.552	2.81	1.273	38.809	.000***
PRS1	Harm to Computers	4.47	1.60	4.41	1.460	1.529	.217
PRS2	Computer Risk	4.54	1.587	4.39	1.457	4.839	.028*
PRS3	Personal Information	4.57	1.584	4.31	1.466	9.696	.002**
PRS4	Personal Privacy	4.39	1.653	4.29	1.510	2.753	.098
PRS5	Threat by Spyware	4.40	1.630	4.34	1.532	1.477	.225
PRS6	Risk of Spyware	4.67	1.612	4.50	1.579	5.034	.025*
Total Perceived Risk of Spyware		4.51	1.471	4.37	1.313	4.671	.031*

TA1	Ability 1	4.46	1.268	4.06	1.350	19.855	.000***
TA2	Ability 2	4.69	1.259	3.91	1.290	70.783	.000***
TA3	Integrity	4.39	1.209	3.86	1.291	35.830	.000***
TA4	Benevolence 1	4.32	1.215	3.59	1.249	66.674	.000***
TA5	Benevolence 2	4.46	1.219	3.77	1.278	60.624	.000***
TA6	Trust	4.40	1.178	3.79	1.283	51.270	.000***
Total Trust of Anti-Spyware Programs		4.45	1.085	3.83	1.120	63.608	.000***
IA1	Likelihood of Use	4.83	1.466	4.20	1.509	39.193	.000***
IA2	Prediction of Use	4.63	1.439	4.24	1.495	18.051	.000***
IA3	Intention to Use	4.69	1.512	4.16	1.517	31.236	.000***
IA4	Recommending to Others	4.57	1.607	3.78	1.475	60.179	.000***
IA5	Multiple Use	4.40	1.541	3.71	1.627	39.843	.000***
Total Intention to Adopt Anti-Spyware Programs		4.62	1.377	4.01	1.330	46.657	.000***

Control variables: age, gender, major, and classification

*p<0.05, **p<0.01, ***p<0.001

Appendix B: Results of Exploratory Factor Analysis (First Result)

Items	Factors (U.S.)							Items	Factors (South Korea)						
	Computer familiarity	Internet Familiarity	Security Familiarity	Knowledge	Perceived Risk	Trust	Intention		Computer familiarity	Internet Familiarity	Security Familiarity	Knowledge	Perceived Risk	Trust	Intention
CF5	**.812**	.162	.222	.111	.130	.126	.175	CF2	**.817**	.043	.217	.274	.094	.031	.010
CF6	**.791**	.182	.305	.102	.128	.174	.142	CF3	**.810**	.073	.259	.239	.097	.083	-.024
CF2	**.766**	.128	.302	.147	.059	.138	.158	CF4	**.797**	.125	.111	.078	.171	.108	.116
CF3	**.766**	.103	.369	.085	.085	.134	.160	CF5	**.792**	.099	.168	.346	.163	.127	.037
CF4	**.766**	.133	.220	.237	.093	.115	.147	CF6	**.761**	.168	.238	.299	.138	.143	.028
CF8	**.710**	.246	.301	.083	.108	.145	.127	CF8	**.717**	.270	.228	.184	.133	.166	.018
CF1	**.649**	.106	.282	.269	.047	.097	.112	CF1	**.697**	.110	.139	-.055	-.019	.006	.178
CF7	*.479*	-.042	.183	.324	.135	.123	.067	CF7	*.499*	-.189	.291	.423	.070	-.020	-.010
IF6	.073	**.870**	.238	-.024	.081	.114	.051	IF6	.074	**.864**	.105	-.077	.130	-.007	.101
IF3	.076	**.861**	.167	.000	.077	.126	.092	IF3	.074	**.850**	.038	-.064	.110	.048	.030
IF2	.084	**.830**	.197	-.086	.115	.120	.099	IF4	.033	**.763**	.133	.028	.025	.069	.105
IF5	.077	**.796**	.117	.011	.138	.103	.067	IF2	.096	**.729**	.090	.002	.139	.153	.037
IF1	.237	**.700**	.050	.098	.069	.169	.104	IF1	.241	**.709**	.005	.119	.105	.167	-.032
IF4	.151	**.651**	.166	.134	.115	-.073	.033	IF5	.053	**.704**	.091	-.057	.154	-.059	.042
SF7	.327	.138	**.848**	.173	.134	.091	.079	SF4	.255	.117	**.881**	.163	.066	.098	.060
SF2	.296	.224	**.826**	.150	.119	.090	.095	SF3	.273	.067	**.844**	.141	.121	.038	.103
SF3	.346	.176	**.819**	.199	.097	.079	.149	SF5	.286	.104	**.835**	.205	.080	.128	.087
SF4	.337	.171	**.803**	.239	.097	.084	.125	SF7	.285	.135	**.835**	.171	.114	.102	.060
SF1	.172	.273	**.791**	.102	.095	.068	.086	SF6	.251	.158	**.823**	.178	.134	.097	.071
SF5	.386	.179	**.787**	.178	.136	.124	.140	SF2	.032	.120	**.721**	.217	.106	.082	.101
SF6	.364	.229	**.779**	.133	.161	.123	.076	SF1	.076	*.437*	.293	.218	.253	.189	.025
KS3	.371	.000	.310	**.665**	.153	.137	.175	KS4	.283	.034	.239	**.813**	.190	.123	.123
KS5	.423	.065	.399	**.624**	.184	.205	.235	KS5	.287	.044	.283	**.766**	.213	.124	.106
KS2	.388	.082	.361	**.613**	.211	.163	.239	KS3	.253	-.130	.278	**.697**	.143	.094	.187
KS1	.358	.028	.389	**.607**	.109	.174	.184	KS2	.259	.101	.249	**.687**	.230	.150	.091
KS4	.422	.061	.354	**.607**	.233	.180	.221	KS1	.242	-.055	.173	**.621**	.118	.158	.315
PRS2	.094	.103	.108	.115	**.877**	.196	.174	PRS3	.114	.108	.103	.088	**.889**	.046	.075
PRS5	.043	.109	.065	.059	**.869**	.145	.178	PRS6	.100	.126	.110	.118	**.867**	.105	.138
PRS3	.194	.132	.157	.095	**.858**	.208	.151	PRS2	.146	.182	.057	.130	**.856**	.032	.112
PRS6	.130	.157	.127	.039	**.849**	.253	.179	PRS5	.093	.114	.136	.071	**.839**	.217	.085
PRS4	.125	.085	.170	.087	**.831**	.178	.138	PRS4	.091	.108	.141	.112	**.838**	.098	.147
PRS1	.054	.109	.055	.138	**.808**	.225	.164	PRS1	.093	.211	.038	.239	**.706**	.127	.133
TA3	.156	.126	.138	.074	.190	**.847**	.184	TA3	.069	.105	.100	.081	.150	**.836**	.266
TA4	.064	.053	.139	.100	.141	**.821**	.178	TA5	.032	.057	.084	.058	.057	**.833**	.259
TA6	.122	.103	.062	.094	.194	**.808**	.316	TA4	.059	-.013	.112	.070	.041	**.819**	.152
TA5	.128	.100	.053	.158	.207	**.807**	.245	TA2	.132	.131	.071	.104	.169	**.811**	.198
TA1	.192	.126	.062	.043	.250	**.780**	.142	TA1	.108	.164	.022	.105	.135	**.808**	.137
TA2	.208	.132	.092	.074	.289	**.763**	.186	TA6	.102	.021	.117	.104	.060	**.791**	.271
IA3	.200	.119	.158	.152	.262	.273	**.800**	IA2	.123	.111	.033	.081	.203	.323	**.843**
IA4	.241	.133	.148	.089	.242	.243	**.776**	IA3	.185	.119	.081	.112	.151	.322	**.819**
IA2	.161	.138	.101	.133	.240	.335	**.773**	IA1	.086	.162	.020	.123	.177	.335	**.810**
IA5	.184	.035	.133	.153	.175	.229	**.773**	IA4	.083	-.008	.167	.092	.148	.306	**.793**
IA1	.188	.151	.122	.133	.237	.347	**.769**	IA5	-.081	.008	.114	.169	.059	.150	**.657**

Second Result

Items	Factors (U.S.)							Items	Factors (South Korea)						
	Computer familiarity	Internet Familiarity	Security Familiarity	Knowledge	Perceived Risk	Trust	Intention		Computer familiarity	Internet Familiarity	Security Familiarity	Knowledge	Perceived Risk	Trust	Intention
CF5	**.809**	.155	.226	.133	.134	.130	.173	CF2	**.814**	.028	.227	.275	.095	.028	.007
CF6	**.790**	.178	.300	.127	.133	.177	.140	CF3	**.808**	.059	.270	.242	.098	.080	-.027
CF2	**.768**	.124	.294	.174	.065	.141	.155	CF4	**.799**	.111	.119	.085	.171	.104	.114
CF4	**.764**	.126	.214	.260	.098	.118	.146	CF5	**.794**	.081	.177	.345	.164	.123	.036
CF3	**.763**	.101	.369	.107	.090	.137	.160	CF6	**.763**	.149	.247	.295	.140	.140	.030
CF8	**.714**	.242	.292	.110	.112	.148	.124	CF8	**.717**	.258	.238	.185	.135	.165	.017
CF1	**.646**	.104	.268	.285	.052	.099	.115	CF1	**.701**	.099	.145	-.039	-.020	.003	.172
IF6	.086	**.875**	.211	-.015	.081	.113	.051	IF6	.078	**.868**	.110	-.065	.135	-.001	.097
IF3	.088	**.865**	.140	.010	.077	.126	.092	IF3	.082	**.853**	.045	-.047	.114	.053	.025
IF2	.090	**.836**	.183	-.084	.115	.120	.102	IF4	.035	**.767**	.138	.037	.030	.075	.103
IF5	.080	**.799**	.103	.003	.138	.103	.073	IF2	.100	**.730**	.095	.005	.144	.158	.038
IF1	.249	**.697**	.024	.121	.072	.171	.097	IF5	.050	**.714**	.096	-.041	.157	-.052	.035
IF4	.152	**.650**	.163	.133	.116	-.072	.034	IF1	.253	**.699**	.011	.120	.109	.168	-.029
SF7	.316	.154	**.853**	.182	.135	.092	.082	SF4	.247	.107	**.885**	.157	.069	.099	.059
SF3	.337	.193	**.817**	.211	.099	.080	.150	SF3	.265	.058	**.849**	.137	.123	.038	.102
SF4	.319	.186	**.815**	.243	.098	.085	.129	SF5	.277	.096	**.841**	.208	.081	.129	.083
SF2	.296	.241	**.807**	.169	.121	.091	.095	SF7	.278	.126	**.840**	.172	.116	.103	.057
SF5	.369	.194	**.801**	.182	.136	.125	.144	SF6	.244	.150	**.828**	.184	.135	.099	.066
SF6	.353	.244	**.785**	.140	.162	.124	.079	SF2	.033	.104	**.721**	.203	.108	.081	.107
KS3	.350	-.001	.310	**.669**	.156	.140	.178	KS4	.279	.020	.248	**.819**	.192	.121	.117
KS5	.406	.064	.402	**.640**	.188	.208	.231	KS5	.286	.026	.291	**.770**	.214	.122	.101
KS2	.376	.082	.352	**.631**	.215	.165	.235	KS3	.239	-.135	.286	**.700**	.144	.094	.180
KS1	.348	.030	.376	**.626**	.113	.176	.181	KS2	.260	.084	.257	**.699**	.231	.148	.084
KS4	.406	.060	.354	**.622**	.236	.183	.218	KS1	.237	-.065	.180	**.624**	.119	.156	.310
PRS2	.091	.103	.099	.120	**.878**	.197	.173	PRS3	.117	.098	.104	.086	**.890**	.046	.076
PRS5	.036	.110	.065	.056	**.869**	.146	.180	PRS6	.096	.124	.113	.123	**.868**	.107	.135
PRS3	.184	.133	.156	.094	**.859**	.209	.154	PRS2	.147	.176	.060	.134	**.857**	.033	.110
PRS6	.123	.158	.126	.040	**.849**	.254	.181	PRS5	.088	.112	.138	.072	**.840**	.219	.084
PRS4	.115	.087	.172	.086	**.832**	.179	.141	PRS4	.091	.099	.142	.111	**.838**	.098	.148
PRS1	.057	.108	.036	.151	**.810**	.226	.160	PRS1	.096	.201	.040	.238	**.707**	.128	.134
TA3	.157	.127	.126	.085	.191	**.848**	.182	TA3	.075	.097	.101	.087	.150	**.836**	.265
TA4	.066	.056	.121	.112	.142	**.820**	.176	TA5	.028	.059	.084	.062	.058	**.835**	.258
TA5	.117	.099	.057	.153	.207	**.808**	.248	TA4	.052	-.008	.114	.075	.041	**.822**	.148
TA6	.113	.104	.061	.090	.193	**.808**	.320	TA2	.141	.118	.071	.102	.169	**.810**	.202
TA1	.184	.123	.071	.041	.250	**.781**	.144	TA6	.106	.012	.117	.105	.060	**.790**	.272
TA2	.196	.130	.105	.070	.288	**.765**	.188	TA1	.114	.156	.023	.106	.136	**.807**	.139
IA3	.195	.120	.153	.160	.262	.273	**.800**	IA2	.128	.106	.034	.085	.203	.321	**.844**
IA4	.235	.135	.145	.092	.242	.243	**.779**	IA3	.192	.110	.083	.114	.151	.319	**.821**
IA5	.175	.036	.135	.151	.175	.229	**.777**	IA1	.094	.155	.021	.130	.177	.333	**.810**
IA2	.158	.138	.095	.140	.240	.336	**.773**	IA4	.081	-.009	.168	.093	.147	.306	**.794**
IA1	.188	.151	.111	.145	.238	.347	**.767**	IA5	-.085	.009	.115	.163	.060	.151	**.660**

Extraction Method: Principal Component Analysis. Rotation Method: Varimax with Kaiser Normalization (Both First and Second).

Appendix C

Technology familiarity and anti-spyware adoption

☞ Questions for Students ☜

Thank you for participating in this study. This study is to examine your technology familiarity, awareness of spyware, and adoption of anti-spyware program. The results will be compared between the U.S. and South Korea. This study is being completed for master's thesis requirements by Dong-Heon Kwak of the Information Systems Department.

The MSU IRB (the committee to protect people who serve as subjects in research) has approved this study (IRB#: 08-10-22).

You must be at least 18 years of age to participate in this study.

If you are under 18 years old, please stop.

Please answer to each question that best applies to you. This survey is anonymous and results will be held in strict confidence. If you have any questions, please contact the researcher, Dong-Heon Kwak (606-207-2717, dhkwak01@morehead-st.edu) or the thesis chair, Dr. Donna Kizzier (606-783-2724, kizzier1234@earthlink.net).

This study will take approximately 10 minutes to complete.

Thank you for your cooperation in advance.

I. The following questions are related to your basic computer experience. Please answer each question by circling the best response or providing the information.

1. Do you use anti-spyware program? (1) Yes (2) No (3) Not sure

2. If you use anti-spyware program, how many programs do you use?

(1) 1 (2) 2 (3) 3 (4) 4 (5) 5 or more (6) Not sure

3. Which operating systems do you use? ***(circle all that apply)***

(1) Microsoft Windows XP (2) Microsoft Windows Vista (3) Mac OS (4) Linux

(5) Solaris (6) Others (please identify) :________________________________

4. How much time do you spend using the computer per day **excluding Internet use?**

(1) less than 1 hour (2) 1 up to 2 hours (3) 2 up to 3 hours

(4) 3 up to 4 hours (5) 4 up to 5 hours (6) more than 5 hours

5. How much time do you spend browsing the Internet per day?

(1) less than 1 hour (2) 1 up to 2 hours (3) 2 up to 3 hours

(4) 3-up to 4 hours (5) 4-up to 5 hours (6) more than 5 hours

II. The following questions are related to your technology familiarity, knowledge and perceived risk of spyware, trust, and intention to adopt anti-spyware program. The example responses follow:

Num	Example Question	Strongly Disagree		←	Neutral	→		Strongly Agree
EX1	I am familiar with online based survey.	1	2	3	4	5	[✓ 6]	7

Num	Example Question	Never Heard		←	Neutral	→		Fully Aware and Know
EX2	What is your general knowledge of rootkit?	1	[✓ 2]	3	4	5	6	7

1. The following questions are **computer familiarity**-related. Please *circle* **(O)** the number that best applies to you.

Num	Questions	Strongly Disagree		←	Neutral	→		Strongly Agree
CF1	I keep up with the latest computer hardware.	1	2	3	4	5	6	7
CF2	I am familiar with changing (installing/upgrading) computer hardware.	1	2	3	4	5	6	7
CF3	I am familiar with computer hardware.	1	2	3	4	5	6	7
CF4	I keep up with the latest computer software.	1	2	3	4	5	6	7
CF5	I am familiar with changing (installing/upgrading) computer software.	1	2	3	4	5	6	7
CF6	I am familiar with computer software.	1	2	3	4	5	6	7
CF7	I enjoy reading computer magazines.	1	2	3	4	5	6	7
CF8	Overall, I am familiar with computers.	1	2	3	4	5	6	7

CONTINUE TO NEXT PAGE ☞

2. The following questions are **Internet familiarity**-related. Please *circle* **(O)** the number that best applies to you.

Num	Questions	Strongly Disagree		←	Neutral	→		Strongly Agree
IF1	I am familiar with the use of search engines.	1	2	3	4	5	6	7
IF2	I am familiar with the use of e-mail.	1	2	3	4	5	6	7
IF3	I am familiar with searching information using the Internet	1	2	3	4	5	6	7
IF4	I am familiar with purchasing products on the Internet.	1	2	3	4	5	6	7
IF5	I am familiar with reading articles on the Internet.	1	2	3	4	5	6	7
IF6	Overall, I am familiar with the Internet.	1	2	3	4	5	6	7

3. The following questions are **security familiarity**-related. Please *circle* **(O)** the number that best applies to you.

Num	Questions	Strongly Disagree		←	Neutral	→		Strongly Agree
SF1	I am familiar with privacy violation issues on the Internet.	1	2	3	4	5	6	7
SF2	I am familiar with technologies which protect people.	1	2	3	4	5	6	7
SF3	I am familiar with security technology.	1	2	3	4	5	6	7
SF4	I am familiar with information security.	1	2	3	4	5	6	7
SF5	I am familiar with computer security.	1	2	3	4	5	6	7
SF6	I am familiar with Internet security.	1	2	3	4	5	6	7
SF7	Overall, I am familiar with general security issues.	1	2	3	4	5	6	7

4. The following questions are **knowledge of spyware**-related. Please *circle* **(O)** the number that best applies to you.

Num	Questions	Strongly Disagree		←	Neutral	→		Strongly Agree
KS1	I update news and developments about the spyware technology.	1	2	3	4	5	6	7
KS2	I know about the problems of malicious software intruding Internet users' computers	1	2	3	4	5	6	7
KS3	I seek advice on computer web sites or magazines about anti-spyware products.	1	2	3	4	5	6	7
KS4	I have knowledge of spyware problems and consequences.	1	2	3	4	5	6	7
KS5	Overall, I have general knowledge of spyware.	1	2	3	4	5	6	7

CONTINUE TO NEXT PAGE ☞

5. The following questions are **perceived risk of spyware**-related. Please ***circle*** **(O)** the number that best applies to you.`

Num	Questions	Strongly Disagree		←	Neutral	→		Strongly Agree
PRS1	I believe that spyware causes significant harm to my computer.	1	2	3	4	5	6	7
PRS2	I believe that my computer is at risk if spyware is downloaded.	1	2	3	4	5	6	7
PRS3	I believe that my personal information is at risk if spyware is downloaded.	1	2	3	4	5	6	7
PRS4	I am concerned about threat to my personal privacy by spyware.	1	2	3	4	5	6	7
PRS5	I am worried about the threat to my computer by spyware.	1	2	3	4	5	6	7
PRS6	Overall, I believe that spyware is risky.	1	2	3	4	5	6	7

6. The following questions are **trust of anti-spyware program**-related. Please ***circle*** **(O)** the number that best applies to you.

Num	Questions	Strongly Disagree		←	Neutral	→		Strongly Agree
TA1	Anti-spyware programs have the ability to remove spyware.	1	2	3	4	5	6	7
TA2	Anti-spyware programs have the ability to protect me from spyware.	1	2	3	4	5	6	7
TA3	Anti-spyware programs are fair in its conduct of computer protection.	1	2	3	4	5	6	7
TA4	Anti-spyware programs consider its users' best interest when working against spyware.	1	2	3	4	5	6	7
TA5	Anti-spyware programs make good-faith efforts to address most user concerns.	1	2	3	4	5	6	7
TA6	Overall, anti-spyware programs are trustworthy.	1	2	3	4	5	6	7

7. The following questions are **intention to adopt anti-spyware program**-related. Please ***circle*** **(O)** the number that best applies to you.

Num	Questions	Strongly Disagree		←	Neutral	→		Strongly Agree
IA1	I am likely to use anti-spyware program.	1	2	3	4	5	6	7
IA2	I predict that I will adopt anti-spyware program.	1	2	3	4	5	6	7
IA3	I intend to periodically use anti-spyware program to protect my computer from spyware.	1	2	3	4	5	6	7
IA4	I will recommend to others that they use anti-spyware program.	1	2	3	4	5	6	7
IA5	I will use two or more anti-spyware programs if helpful.	1	2	3	4	5	6	7

CONTINUE TO NEXT PAGE ☞

8. The following questions are **specific features of spyware -related**. Please *circle* **(O)** the number that best applies to you.

Num	Questions	Never Heard		←	Neutral	→		Fully Aware and Know
SFS1	What is your knowledge that spyware can trace keystrokes?	1	2	3	4	5	6	7
SFS2	What is your knowledge that spyware can reside on computer?	1	2	3	4	5	6	7
SFS3	What is your knowledge that spyware can monitor surfing behavior?	1	2	3	4	5	6	7
SFS4	What is your knowledge that spyware can record online transactions?	1	2	3	4	5	6	7
SFS5	What is your knowledge that spyware can be used as denial of service (DOS) attack?	1	2	3	4	5	6	7
SFS6	What is your knowledge of how spyware is installed?	1	2	3	4	5	6	7

Your responses to the following questions will be held in strict confidence and your anonymity will be protected. The following items will be reported only in composite form for analysis purposes. Individual responses cannot be singled out.

III. The following is demographic questions. Please answer the each question by circling the best response or providing the information.

1. What is your gender? (1) Male (2) Female
2. What is your major? ( )
3. Your classification? (1) Freshman (2) Sophomore (3) Junior
(4) Senior (5) Graduate (6) Others ( )
4. How old are you? ( )
5. Your citizenship? (1) U.S. (2) Others ( )

After finishing the survey, please put it in the envelope in front of the instructor.

Thank you for your participation.

Contact Information
Dong-Heon Kwak (606-207-2717, dhkwak01@morehead-st.edu)
Thesis Chair, Dr. Donna Kizzier (606-783-2724, kizzier1234@earthlink.net)

Appendix D

안티스파이웨어 프로그램의 사용에 관한 분석을 위한 질문

☞ 학생용 설문지 ☜

안녕하십니까?

먼저 본 질문지에 응해 주셔서 진심으로 감사드립니다.

본 연구는 각 개인의 기술 친숙도, 스파이웨어 인지, 그리고 안티 스파이웨어 프로그램에 대한 신뢰도를 간의 관계를 탐색하여 개인의 안티 스파이웨어 프로그램 사용에 영향을 주는 요인의 발견하기 위한 것입니다. 여러분의 귀중한 자료는 미국과의 비교연구로도 활용될 것입니다.

각 문항의 내용이 여러분 개개인과 어느 정도 일치하는지 응답해 주시면 됩니다. 바쁘시더라도 한 문항도 빠짐없이 응답해 주시면 감사하겠습니다. 본 질문지는 연구의 목적으로만 사용할 것임을 약속드립니다. 귀하의 답변은 엄격히 비밀로 지켜질 것이며 여러분의 익명성도 보장될 것입니다. 혹시 질문이 있으시면 다음 연락처로 문의 바랍니다.

곽동헌 (1-606-207-2717, dhkwak01@morehead-st.edu),

논문지도교수 Dr. Donna Kizzier (606-783-2724, kizzier1234@earthlink.net)

본 연구는 대략 10분 정도 소요될 예정입니다.

여러분의 협조에 미리 감사드립니다.

2008년 10월

Morehead State University

Information Systems Department

I. 다음은 여러분의 컴퓨터 경험에 관한 질문입니다. 해당 부분에 O표를 하시거나 알맞은 답을 적어주시기 바랍니다.

1. 당신은 안티스파이웨어 프로그램을 사용합니까? (1) 예 (2) 아니오 (3) 잘 모르겠다.

2. 만약 안티스파이웨어 프로그램을 사용한다면, 몇 개의 프로그램를 사용하십니까?

(1) 1개 (2) 2개 (3) 3개 (4) 4개 (5) 5개 이상 (6) 잘 모르겠다

3. 당신은 어떤 운영체제를 사용하십니까? (해당사항에 모두 응답해 주세요)

(1) MS 윈도우 XP (2) MS 윈도우 비스타 (3) 맥킨토시 운영체제 (4) 리눅스
(5) 솔라리스 (6) 기타 ( )

4. 하루에 얼마나 컴퓨터를 사용하십니까? (인터넷 사용시간제외)

(1) 1시간 미만 (2) 1시간 이상 - 2시간 미만 (3) 2시간 이상 - 3시간 미만

(4) 3시간 이상 - 4시간 미만 (5) 4시간 이상 - 5시간 미만 (6) 5시간 이상

5. 하루에 얼마나 인터넷을 사용하십니까?

(1) 1시간 미만 (2) 1시간 이상 - 2시간 미만 (3) 2시간 이상 - 3시간 미만

(4) 3시간 이상 - 4시간 미만 (5) 4시간 이상 - 5시간 미만 (6) 5시간 이상

II. 다음 문항은 여러분의 컴퓨터 친숙도, 스파이웨어 지식과 지각된 위협, 안티스파이웨어 프로그램에 대한 신뢰, 안티스파이웨어 프로그램 사용의도를 알아보기 위한 질문입니다. 아래 예시와 같이 응답해 주세요.

예 시

번호	예시 질문	전혀 그렇지 않다			← 보통이다 →			매우 그렇다
EX1	나는 온라인 설문에 익숙하다.	1	2	3	4	5	[✓ 6]	7

1. 다음 문항은 컴퓨터 친숙도에 대한 질문입니다. 각 문항의 일치하는 곳에 O표를 해 주세요.

번호	문항	전혀 그렇지 않다			← 보통이다 →			매우 그렇다
CF1	나는 최신의 컴퓨터 하드웨어를 유지한다.	1	2	3	4	5	6	7
CF2	나는 컴퓨터 하드웨어를 바꾸는데 (설치,향상) 익숙하다.	1	2	3	4	5	6	7
CF3	나는 컴퓨터 하드웨어에 익숙하다.	1	2	3	4	5	6	7
CF4	나는 최신의 컴퓨터 소프트웨어를 유지한다.	1	2	3	4	5	6	7
CF5	나는 컴퓨터 소프트웨어를 바꾸는데 (설치,향상) 익숙하다.	1	2	3	4	5	6	7
CF6	나는 컴퓨터 소프트웨어에 익숙하다.	1	2	3	4	5	6	7
CF7	나는 컴퓨터관련 잡지를 읽는 것을 즐긴다.	1	2	3	4	5	6	7
CF8	전체적으로 나는 컴퓨터에 익숙하다.	1	2	3	4	5	6	7

다음 페이지에 계속 ☞

2. 다음 문항은 인터넷 친숙도에 대한 질문입니다. 각 문항의 일치하는 곳에 O표를 해 주세요.

번호	문항	전혀 그렇지 않다			← 보통이다 →			매우 그렇다
IF1	나는 검색엔진 사용에 익숙하다.	1	2	3	4	5	6	7
IF2	나는 이메일 사용에 익숙하다.	1	2	3	4	5	6	7
IF3	나는 인터넷을 사용해서 정보검색하는 것에 대해 익숙하다.	1	2	3	4	5	6	7
IF4	나는 인터넷에서 상품을 구입하는데 익숙하다.	1	2	3	4	5	6	7
IF5	나는 인터넷에서 신문 기사를 읽는데 익숙하다.	1	2	3	4	5	6	7
IF6	전체적으로 나는 인터넷에 익숙하다.	1	2	3	4	5	6	7

3. 다음 문항은 보안 친숙도에 대한 질문입니다. 각 문항의 일치하는 곳에 O표를 해 주세요.

번호	문항	전혀 그렇지 않다			← 보통이다 →			매우 그렇다
SF1	나는 인터넷 상에서의 사생활 침해 문제에 관해 익숙하다.	1	2	3	4	5	6	7
SF2	나는 사람들을 보호하는 기술에 대해 익숙하다.	1	2	3	4	5	6	7
SF3	나는 보안 기술에 익숙하다.	1	2	3	4	5	6	7
SF4	나는 정보 보안에 익숙하다.	1	2	3	4	5	6	7
SF5	나는 컴퓨터 보안에 익숙하다.	1	2	3	4	5	6	7
SF6	나는 인터넷 보안에 익숙하다.	1	2	3	4	5	6	7
SF7	전체적으로 나는 일반 보안문제에 대해 익숙하다.	1	2	3	4	5	6	7

4. 다음 문항은 스파이웨에 지식에 대한 질문입니다. 각 문항의 일치하는 곳에 O표를 해 주세요.

번호	문항	전혀 그렇지 않다			← 보통이다 →			매우 그렇다
KS1	나는 스파이웨어와 관련된 뉴스를 업데이트한다.	1	2	3	4	5	6	7
KS2	나는 인터넷 사용자들의 컴퓨터에 침입하는 악성 소프트웨어의 문제에 관해 안다.	1	2	3	4	5	6	7
KS3	나는 안티 스파이웨어 제품과 관련된 의견(조언)을 컴퓨터 웹사이트나 잡지에서 찾는다.	1	2	3	4	5	6	7
KS4	나는 스파이웨어 문제와 결과에 대한 지식을 가지고 있다.	1	2	3	4	5	6	7
KS7	전체적으로 나는 스파이웨어에 관해 일반적 지식을 가지고 있다.	1	2	3	4	5	6	7

5. 다음 문항은 스파이웨어에 관한 인식된 위험에 대한 질문입니다. 각 문항의 일치하는 곳에 O표를 해 주세요.

번호	문항	전혀 그렇지 않다			← 보통이다 →			매우 그렇다
PRS1	나는 스파이웨어가 내 컴퓨터에 심각한 손상을 일으킨다고 믿는다.	1	2	3	4	5	6	7
PRS2	나는 스파이웨어가 설치된다면 내 컴퓨터가 위험하다고 믿는다.	1	2	3	4	5	6	7
PRS3	나는 스파이웨어가 설치된다면 내 개인정보가 위험하다고 믿는다.	1	2	3	4	5	6	7
PRS4	나는 스파이웨어에 의해 내 개인 프라이버시가 위협받는 것에 관해 염려한다.	1	2	3	4	5	6	7
PRS5	나는 스파이웨어에 의해 내 컴퓨터가 위협받는 것에 관해 걱정한다.	1	2	3	4	5	6	7
PRS6	전체적으로 나는 스파이웨어가 위험하다고 믿는다.	1	2	3	4	5	6	7

6. 다음 문항은 안티스파이웨어 프로그램의 신뢰성에 대한 질문입니다. 각 문항의 일치하는 곳에 O표를, 해 주세요.

번호	문항	전혀 그렇지 않다			← 보통이다 →			매우 그렇다
TA1	안티스파이웨어 프로그램은 스파이웨어를 제거할 수 있는 능력을 가지고 있다.	1	2	3	4	5	6	7
TA2	안티스파이웨어 프로그램은 스파이웨어로부터 나를 보호할 수 있는 능력을 가지고 있다.	1	2	3	4	5	6	7
TA3	안티스파이웨어 프로그램은 컴퓨터보호 임무에 적당하다.	1	2	3	4	5	6	7
TA4	안티스파이웨어 프로그램은 스파이웨어에 대항해서 작동하는 동안 사용자의 이익을 최대한 고려한다.	1	2	3	4	5	6	7
TA5	안티스파이웨어 프로그램은 대부분 사용자의 염려를 덜어주려는 선의의 노력을 한다.	1	2	3	4	5	6	7
TA6	전체적으로 안티스파이웨어 프로그램은 신뢰할만하다.	1	2	3	4	5	6	7

7. 다음 문항은 안티스파이웨어 프로그램의 사용의도에 대한 질문입니다. 각 문항의 일치하는 곳에 O표를 해 주세요.

번호	문항	전혀 그렇지 않다			← 보통이다 →			매우 그렇다
IA1	나는 안티스파이웨어 프로그램을 사용할 것 같다.	1	2	3	4	5	6	7
IA2	나는 안티스파이웨어 프로그램을 사용할 것이라고 예상한다.	1	2	3	4	5	6	7
IA3	나는 내 컴퓨터를 스파이웨어로부터 보호하기 위해 주기적으로 안티스파이웨어 프로그램을 사용할 것이다.	1	2	3	4	5	6	7
IA4	나는 다른 사람들에게 안티스파이웨어 프로그램을 사용할 것을 권유할 것이다.	1	2	3	4	5	6	7
IA5	만약 도움이 된다면 나는 두 개 이상의 안티스파이웨어 프로그램을 사용할 것이다.	1	2	3	4	5	6	7

다음 페이지에 계속 ☞

8. 다음 문항은 스파이웨어의 구체적 특성에 대한 지식과 관련된 질문입니다. 각 문항의 일치하는 곳에 O표를 해 주세요.

번호	문항	전혀 들어본적 없다			← 보통이다 →			매우 잘 안다
SKS1	스파이웨어가 키스트로크(keystroke)* 를 추적(기록) 할수 있다는 것에 관해 알고 있습니까? * 키스트로크: 컴퓨터 키보드를 누르는 행위	1	2	3	4	5	6	7
SKS2	스파이웨어가 컴퓨터에 존재할 수 있다는 것에 관해 알고 있습니까?	1	2	3	4	5	6	7
SKS3	스파이웨어가 사용자의 웹서핑을 감시할 수 있다는 것에 관해 알고 있습니까?	1	2	3	4	5	6	7
SKS4	스파이웨어가 사용자의 온라인거래를 기록할 수 있다는 것에 관해 알고 있습니까?	1	2	3	4	5	6	7
SKS5	스파이웨어가 서비스 거부 (DOS) 공격*으로 사용될 수 있다는 것에 관해 알고 있습니까? * 서비스거부 공격: 비정상적으로 컴퓨터 리소스의 소모를 발생시키 위한 시도	1	2	3	4	5	6	7
SKS7	어떻게 스파이웨어가 설치되는지 알고 있습니까?	1	2	3	4	5	6	7

아래 질문에 관한 귀하의 답변은 엄격히 비밀로 지켜질 것이며 여러분의 익명성도 보장될 것입니다. 또한 아래 질문은 단지 분석의 목적으로만 사용될 것이며 개개인의 응답은 따로 사용되지 않을 것입니다.

III. 다음은 개인 신상에 관한 질문입니다. 알맞은 답을 적어 주시기 바랍니다.

1. 당신의 성별은? (1) 남 (2) 여

2. 당신의 전공은? ( )

3. 몇 학년입니까? (1) 1학년 (2) 2학년 (3) 3학년 (4) 4학년 (5) 대학원생

4. 당신의 나이는? ( )

여러분의 참여에 감사드립니다.

연락정보

곽동헌 (1-606-207-2717, dhkwak01@morehead-st.edu)

Dr. Donna Kizzier (606-783-2724, kizzier1234@earthlink.net)

MSU Institutional Review Board for the Protection of Human Subjects in Research
NOTIFICATION OF PROTOCOL REVIEW

Principal Investigator/Researcher:

Name: Dong-Heon Kwak, Donna Kizzier   Title: Masters student

Campus Address: 320 Combs   Campus Phone: 606-207-2717

Department: Department of Information Systems

Purpose:

Title of Project/Course: From technology familiarity to anti-spyware program adoption: comparison between U.S. and South Korea

Funding Source/Agency: N/A

Period of Project/Course: From: 10/27/08 To: 10/26/09

Protocol Review Number: 08-10-22

Initial Review X   Continuing Review ____

The human subject use protocol described above has been reviewed by the MSU Institutional Review Board for the Protection of Human Subjects in Research with the following results:

Yes ☒ No □ Approved, may proceed as written

10/27/08 Approval Period

10/27/08 - 10/26/09 Approval for Continuing Review must be received prior to date shown

Yes □ No □ N/A ☒ Regulatory requirements have been met for the waiver of informed consent

Yes ☒ No □ N/A □ Regulatory requirements have been met for the waiver of documentation of consent

Yes □ No □ N/A ☒ Criteria for use of children, prisoners, pregnant women has been met

Signed: ______________________ Date: 10/27/08
Chair, Institutional Review Board for the Protection of Human Subjects in Research

'lease refer to the protocol review number in any future references to this protocol. Principal investigators of research projects vith durations of more than one year should submit yearly to the IRB completed Form H; if *any* revisions are made to a project r if *any* unforeseen risks arise during an investigation, the principal investigator must submit Form H to the IRB, fully explaining ll changes or unexpected risks; upon completion or termination of a research project, principal investigators must again submit orm H.