Spyware: What Influences College Students to Use Anti-Spyware Tools?

Michael R. Ward
wardmr@appstate.edu

D. Scott Hunsinger
hunsingerds@appstate.edu
Department of Computer Information Systems
Appalachian State University
Boone, NC 28608-2037, United States

ABSTRACT

Spyware has become a major problem in businesses, schools, and homes today and is often discussed by reliable news and trade magazines. Significant research has been done on spyware and the damaging effects that it has on computers and people. With the wide range of information available for the public to obtain, why are there so many people who still do not protect their computers from spyware? To begin to answer these questions, we first reviewed several theories used to determine what factors influence people to perform a certain behavior. We examined the Theory of Planned Behavior and the Technology Acceptance Model. We decided to limit the scope of our paper to college students since this sample was more readily available to us than the general public. The purpose of this paper is to better understand what factors influence college students to run anti-spyware tools, with the hopes of finding ways to better inform future students about the spyware epidemic and ways to combat spyware. In order to determine what influences students to use anti-spyware tools, we conducted multiple structured interviews (n=10) and a survey (n=68). These provided insight into the factors influencing students to run anti-spyware tools. We also found significant differences between Computer Information Systems (CIS) majors and non-CIS majors in their usage of anti-spyware software. Our research suggests that Attitude, Perceived Behavioral Control, and Technology Awareness have the most impact on influencing a college student's intentions to use anti-spyware tools.

Keywords: Spyware, Theory of Planned Behavior, Behavioral Intention, Attitude, Perceived Behavioral Control, Technology Awareness

1. INTRODUCTION

Spyware is defined as "software that is installed on a computer without the user's knowledge and transmits information about the user's computer activities over the Internet" (Spyware, 2009). Spyware is becoming a rapid threat to productivity and revenue in today's technological world. U.S. consumers spent $2.6 billion during 2006 to prevent or remove spyware (I-SPY, 2007). They lost almost $8.5 billion and replaced about 2.1 million computers between 2007 and 2008 due to viruses, spyware, and phishing scams (Consumer Reports, 2008). Spyware causes computers to suffer in performance and can steal information from consumers, which can lead to identity theft or software failure. Microsoft, in fact has stated that spyware is "at least partially responsible for approximately one-half of ap-

plication crashes reported to them" (I-SPY, 2007).

Spyware is a growing problem that is impacting the average consumer and business today. However, the average consumer seems to do nothing with the information made available to them about spyware. About 75% of Internet users know about spyware, but only about 70% of these Internet users know about the importance of installing anti-spyware tools (Chenoweth et al., 2009). However, the 70% of Internet users who know about the importance of anti-spyware tools still often do nothing about it (Chenoweth et al., 2009). Studies have shown that most spyware problems that occur today could be prevented with anti-spyware tools (Lee and Kozar, 2005). Even though the studies have suggested that having the right tools can prevent a large number of spyware problems, there is still just a 10% adoption rate of anti-spyware software (Lee and Kozar, 2005).

With all of the information available about spyware, it is unclear why people are not doing more to protect themselves from it. With the ever-growing threat of spyware, people are less likely to put their trust in online websites such as e-commerce sites that ask for their personal information (I-SPY, 2007).

Why doesn't the average consumer try to prevent the likelihood of a spyware-related attack? To try to answer this question, we are going to examine the factors influencing college students to run anti-spyware tools. We will also examine the differences between responses of Computer Information Systems (CIS) majors and non-CIS majors to gain a better understanding of which factors are most influential for each group.

The remainder of the paper is structured as follows: The literature review section provides statistics from previous studies relating to spyware and reviews several relevant theories. We state our hypotheses in Section 3. The methodology section explains how we captured both qualitative and quantitative data for our analysis and provides information about our measures. In the findings section, we provide the results of our analysis. The discussion and conclusion sections provide suggestions based upon our findings for addressing the growing problem of spyware.

2. LITERATURE REVIEW

Spyware Statistics

A study conducted by the National Cybersecurity Alliance stated, "…over 90 percent of consumers had some form of spyware on their computers and most consumers were not aware of it" (I-SPY, 2007). Businesses are also impacted by spyware. Over 90 percent of PC's in large organizations have spyware on them; some studies have found that computers have an average of 28 different types of spyware on them (Chenoweth et al., 2009). Spyware has become a huge threat to companies due to losses in productivity and potential data loss. Security vulnerabilities have risen from less than 1,100 in the year 2000 to over 7,000 in the year 2007, according to the CERT Coordination Center (I-SPY, 2007).

Even the most popular websites perceived to be safe often contain spyware. "70 percent of the top 100 websites either hosted malicious content or contained a link designed to redirect site visitors to a malicious web site during the second half of 2008 . . ." (Claburn, 2009). The article also mentioned that "77 percent of websites with known malicious code are 'legitimate' sites".

The US government proposed legislation to crack down on spyware creators. The government's proposed amendment would enforce criminal penalties on the distribution of spyware. The legislation will impose a "maximum of 2 years for using spyware to break into a computer and alter the security settings or obtain personal information about a person" (I-SPY, 2007).

Catching these criminals can be very difficult, because they are adapting how they distribute spyware. Spyware is being disseminated today from sites that are appearing on the Internet for very short periods of time. From October 2008 to January 2009, the number of new malicious sites increased from 100,000 to 200,000 per day to 200,000 to 300,000 per day (Seltzer, 2009). These sites come up as quickly as they go down. Sixty-two percent (62%) of fake codec sites, perhaps the most dangerous form of spyware, are active for less than a day (Seltzer, 2009). With sites appearing and disappearing this quickly, it makes it very difficult to trace the person(s) responsible for them. Even though spyware may never

be eliminated completely, there are ways to protect against it.

Background Theories

Several theories can be used to explain what influences a college student's intention to adopt anti-spyware software. These theories use certain criteria that can help us determine the factors influencing a person to use and maintain protective technologies. Protective technologies are technologies that help to protect or combat malicious programs that can be installed on a computer (Chenoweth et al., 2009). Several theories, including the Theory of Planned Behavior and the Technology Acceptance Model, may be used to help us better understand the usage of anti-spyware software.

Theory of Planned Behavior

The Theory of Planned Behavior (TPB), introduced by Ajzen (1991), "…contends that a person's behavior is determined by his or her intention to perform the behavior of interest" (Dinev and Hu, 2007). A number of other researchers have used the TPB to determine what influences people to perform certain behaviors (Larose et al., 2009; Rawstorne et al., 2000; Sipior and Ward, 2008). The Theory of Planned Behavior uses Attitude towards the behavior, Subjective Norm, and Perceived Behavioral Control as predictors of Behavioral Intention (Ajzen, 1991). The traditional Theory of Planned Behavior is illustrated in Figure 1.

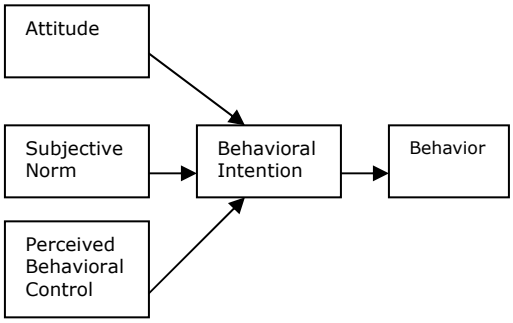

Figure 1: Theory of Planned Behavior (after Ajzen, 1991)

Researchers have suggested additional constructs to add to the predictive power of the Theory of Planned Behavior. Some researchers have added constructs to try to better understand what influences people to adopt protective technologies.

Dinev and Hu (2007) introduced additional constructs to the PBC: Self-efficacy (SE) and Controllability (C). Self-efficacy is defined as "…the individual judgments of person's skills and capabilities to perform the behavior," and Controllability is the "individual's judgments about the availability of resources and opportunities to perform the behavior" (Dinev and Hu, 2007). They introduced these constructs to determine if people were more likely to use the anti-spyware tools if they believed they had the capabilities to perform the task and if they had the available resources to get the tools.

Dinev and Hu (2007) also added the Technology Awareness construct to their study. Technology Awareness is defined as "the user's following and being interested in and knowledgeable about technological issues, problems and strategies to solve them" (Dinev and Hu, 2007). The Theory of Planned Behavior has been used in its original form and/or has had constructs added to it in order to better determine people's intentions to adopt protective technologies.

Technology Acceptance Model

"The Technology Acceptance Model (TAM) (Davis, 1989) has been widely used to predict an individual's intentions to adopt technology. TAM's main variables include Perceived Ease of Use (PEOU), Perceived Usefulness (PU), and Attitude (A). "PEOU is defined as the degree to which the user expects that usage requires limited effort" and "PU is the degree to which a person believes that using a particular system would enhance his or her job performance within an organizational context" (Dinev and Hu, 2007). TAM's constructs help to predict people's intentions to adopt technologies. Kumar et al. (2008) applied this model to determine people's intentions to use firewalls, a type of protective technology. Through Kumar et al.'s (2008) research, they found that a person's attitude towards firewalls is a good indicator that they will go through with their intentions to implement a firewall.

Lee et al. (2008) added Self-identity to TAM to demonstrate the voluntary aspect of social influence. Their study confirmed the significant influence of Self-Identity to technology acceptance, finding that it enables us to capture a distinct social influence on technology acceptance in situations where

Subjective Norm is not able to do so (Lee et al., 2008). TAM has shown to be a strong predictor of acceptance of new technologies.

Dinev and Hu (2007) combined parts of the Technology Acceptance Model with the Theory of Planned Behavior (TPB). They added the TAM to the TPB because they wanted to incorporate the Perceived Ease of Use and the Perceived Usefulness constructs.

3. HYPOTHESES

The traditional constructs in the Theory of Planned Behavior are Attitude, Subjective Norm, and Perceived Behavioral Control (Ajzen, 1991). A person's intention to perform the behavior in question (in this case, to use anti-spyware software), is stronger when Attitude and Subjective Norm are more favorable and Perceived Behavioral Control is greater (Davis, Ajzen, et al, 2002).

Therefore, our first three hypotheses are:

- **Hypothesis 1**: Attitude is positively correlated with Behavioral Intention to use anti-spyware tools.
- **Hypothesis 2**: Subjective Norm is positively correlated with Behavioral Intention to use anti-spyware tools.
- **Hypothesis 3**: Perceived Behavioral Control is positively correlated with Behavioral Intention to use anti-spyware tools.

Our study adds a fourth predictor, Technology Awareness, as originally suggested by Dinev and Hu (2007).

- **Hypothesis 4**: Technology Awareness is positively correlated with Behavioral Intention to use anti-spyware tools.

4. METHODOLOGY

First, we collected information from the computer walk-in center at our university, which is a branch of Technology Support Services. We then created an interview instrument using the Theory of Planned Behavior (Ajzen, 2001) to guide our questions. We randomly selected five CIS majors and five non-CIS majors to interview (instrument available in Appendix). We conducted structured interviews to investigate students' attitudes, beliefs, thoughts, and concerns about using anti-spyware software. All interviews were taped and transcribed.

Based upon the interview data and statements used to measure constructs from previous Theory of Planned Behavior research, we created our instrument. The survey also included statements related to the Technology Awareness construct found in the Dinev and Hu (2007) study.

We used Survey Monkey for hosting purposes. Each of the questions in the survey allowed the respondents to answer on a seven-point Likert scale ranging from Strongly Agree (1) to Strongly Disagree (7).

Measures

Behavioral Intention

Two statements were used to measure Behavioral Intention: (BI1) I plan to use anti-spyware tools, and (BI2) I intend to use anti-spyware tools. Cronbach's alpha = .861 for Behavioral Intention.

Attitude

We used three statements to measure Attitude toward the behavior: (ATT1) Adopting anti-spyware software is a *good* idea; (ATT2) Adopting anti-spyware software is a *positive* idea; and (ATT3) Adopting anti-spyware software is a *beneficial* idea. Cronbach's alpha = .882 for Attitude.

Subjective Norm

Two statements were used to measure Subjective Norm: (SN1) The people who are important to me adopt anti-spyware software, and (SN2) The people whose opinions I value adopt anti-spyware software. Cronbach's alpha = .80 for Subjective Norm.

Perceived Behavioral Control

We used several statements generated from the interview data and/or used in previous TPB research to measure Perceived Behavioral Control: (PBC1) I will be able to adopt anti-spyware software if I choose to do so; (PBC2) Adopting anti-spyware software is entirely within my control; (PBC3) I have the resources to adopt anti-spyware software; (PBC4) I have the knowledge to adopt anti-spyware software; (PBC5) I have the ability to adopt anti-spyware software; and (PBC6)

I have the time to adopt anti-spyware software. Cronbach's alpha = .902 for this construct.

Technology Awareness

Five statements used in Dinev and Hu's study (2007) were included in our survey instrument: (TA1) I follow news and developments about spyware technology; (TA2) I discuss with friends and people around me security issues of the Internet; (TA3) I read about the problems of malicious software intruding Internet users' computers; (TA4) I seek advice on computer web sites or magazines about anti-spyware products; and (TA5) I am aware of the spyware problems and consequences. Cronbach's alpha = .805 for Technology Awareness.

Factor Analysis

We conducted a factor analysis as shown in Figure 2 using principal component analysis and varimax rotation. The rotation converged in seven iterations. In Figure 2, ATT = Attitude; SN = Subjective Norm; PBC = Perceived Behavioral Control; and TA = Technology Awareness.

	COMPONENT			
	ATT	**SN**	**PBC**	**TA**
ATT1	.722			
ATT2	.855			
ATT3	.876			
SN1		.911		
SN2		.848		
PBC1			.588	
PBC2			.758	
PBC3			.829	
PBC4			.738	
PBC5			.781	
PBC6			.743	
TA1				.705
TA2				.841
TA3				.765
TA4				.599
TA5				.577

Figure 2: Factor Analysis

Demographics

We invited 104 students taking select classes in the College of Business at our university to participate. Sixty-eight (68) students completed the survey, resulting in a response rate of 65%.

The respondents to the survey were comprised of 38.2% Computer Information Systems (CIS) majors and 61.8% non-CIS majors. The survey included 69.7% males and 30.3% females. The class distribution is shown in Table 1.

Table 1: Class Distribution

Year of College	Percent of Total
Sophomore	8.8%
Junior	29.4%
Senior	61.8%

5. FINDINGS

Technology Support Services

In order to get a better overall understanding of the usage of anti-spyware tools at our university, we spoke with the director of the walk-in center for students and faculty. The director agreed to see how many of the computers brought in by students that day contained spyware. Twenty-eight percent (28%) or nine computers out of thirty-two had spyware on them. These nine computers with spyware had a total of **16,447** instances of spyware! This number was so large that we asked the director how much of their work involved spyware. He estimated that about seventy-five percent (75%) of their work resulted directly from spyware problems. The numbers that we gathered from just one day were remarkable. This shows that there are still a lot of students who do not use anti-spyware programs. This also suggests that there are still students who do not know about spyware and its effects.

Interview and Survey Findings

We gathered quantitative information from the survey and qualitative information from the interviews done with the students. We analyzed the quantitative information from the survey and the qualitative information from each interview. We used the data to determine the main constructs that stood out from the research. The main constructs

that stood out from the survey and the interviews were Perceived Behavioral Control, Technology Awareness, and Attitude towards adopting anti-spyware tools. However, the construct of Subjective Norm seemed to not hold as much importance.

We used SPSS to compare the means for CIS majors and non-CIS majors for each construct using one-way ANOVA. For all constructs, we used a seven-point Likert scale in which 1 = Strongly Agree and 7 = Strongly Disagree.

Behavioral Intention

When interviewing CIS majors, we found that all of them intend to use anti-spyware tools, which falls into the Behavioral Intention construct. This group already knew the importance of using anti-spyware tools. Even though most non-CIS majors also intended to use anti-spyware software, we found significant differences between intentions of CIS and non-CIS students.

Table 2 summarizes the survey results of the data analysis for both CIS and non-CIS majors (1 = Strongly Agree; 7 = Strongly Disagree).

Table 2: Behavioral Intention

Statement	CIS Avg	Non-CIS Avg	F
I plan to use anti-spyware tools	1.22	2.00	8.418**
I intend to use anti-spyware tools	1.22	1.74	5.289*

*p < .05; **p<.01

Perceived Behavioral Control

We examined whether students possessed volitional control over using anti-spyware tools, which involves the construct of Perceived Behavioral Control. The interview and survey results revealed that most students agreed that they had control over using anti-spyware tools. However, CIS majors believed they had more control than non-CIS majors.

We asked the interviewees if they had the knowledge, resources, and ability to adopt the anti-spyware tools. One of the interviewees said, "Yes, I feel I'm experienced enough to implement, update and maintain anti-spyware." The CIS majors we interviewed use anti-spyware tools and said they have the knowledge, resources, and ability to use the tools. When we asked the non-CIS students if they used anti-spyware tools it was not a unanimous yes.

As shown in Table 3, we found significant differences from our survey results between the CIS and non-CIS majors for most statements relating to the Perceived Behavioral Control construct. (1 = Strongly Agree; 7 = Strongly Disagree)

Table 3: Perceived Behavioral Control

Statement	CIS Avg	Non-CIS Avg	F
I will be able to adopt anti-spyware software if I choose to do so	1.83	2.00	.509 (ns)
Adopting anti-spyware software is entirely within my control	1.50	2.21	10.163**
I have the resources to adopt anti-spyware software	1.45	2.38	11.910**
I have the knowledge to adopt anti-spyware software	1.41	2.80	21.971***
I have the ability to adopt anti-spyware software	1.66	2.21	4.831*
I have the time to adopt anti-spyware software	1.91	2.88	9.854**

*p < .05; **p<.01; ***p<.001

ns = not significant

Technology Awareness

During an interview with one of the students, we asked her if she used anti-

spyware tools. She said, "I don't think so." As we further talked with her, we realized that she did not know about spyware at all. The statements from this interviewee relate to the Technology Awareness construct. Awareness of spyware and anti-spyware tools is greater for CIS majors than non-CIS majors. We asked the CIS majors how they learned about spyware and anti-spyware tools. Their knowledge came from personal experiences, classes, and work. One of the interviewees said they learned about spyware "through personal research and at work." The non-CIS majors who used anti-spyware tools stated in the interviews that they learned about the tools through family or just reading websites. The survey data also showed that awareness is an important construct in influencing individuals to use anti-spyware tools.

Table 4 summarizes the results of the survey data analysis for both CIS and non-CIS majors (1 = strongly agree; 7 = strongly disagree).

Attitude

The feeling of safety experienced from using anti-spyware tools relates to students' attitudes and perceptions toward these tools. The Attitude construct was examined when we asked the interviewees if they felt if the anti-spyware tools were an inconvenience or a hassle to them. Most of the interviewees said they that the tools were not an inconvenience.

However, one of the interviewees said, "I see it as a hassle when it slows my computer down, but it's probably worth it." This statement shows a negative connotation toward the use of anti-spyware tools. There were only two interviewees that expressed a negative attitude toward these tools, however.

Table 5 displays the three statements used to measure the Attitude construct. No significant differences were found for this construct between CIS and non-CIS majors.

Table 4: Awareness

Statement	CIS Avg	Non-CIS Avg	F
I follow news and developments about spyware technology	3.04	4.61	15.504***
I discuss with friends and people around me security issues of the Internet	2.91	3.73	4.458*
I read about the problems of malicious software intruding Internet users' computers	2.00	2.88	6.631*
I seek advice on computer web sites or magazines about anti-spyware products	2.95	3.90	4.849*
I am aware of the spyware problems and consequences	1.75	2.78	11.706**

*p < .05; **p<.01; ***p<.001

Table 5: Attitude

Statement	CIS Avg	Non-CIS Avg	F
Adopting anti-spyware software is a good idea	1.71	1.92	.993 (ns)
Adopting anti-spyware software is a positive idea	1.88	1.98	.253 (ns)
Adopting anti-spyware software is a beneficial idea	1.96	2.12	.364 (ns)

ns = not significant

Subjective Norm

Overall, the non-CIS interviewees indicated that they were not influenced by other

people who used anti-spyware tools. These findings suggest that subjective norm has less effect in influencing a student to adopt the use of anti-spyware tools. Some of the interviewees were influenced by family and friends, but a lot of them said, "No, I have made these decisions on my own."

The survey data is in line with the interviews, as many students (especially non-CIS majors) responded neutrally to the statements dealing with subjective norm. Table 6 shows that no significant differences exist between CIS and non-CIS majors for Subjective Norm.

Table 6: Subjective Norm

Statement	CIS Avg	Non-CIS Avg	F
The people who are important to me adopt anti-spyware software.	3.08	3.26	.339 (ns)
The people whose opinions I value adopt anti-spyware software.	3.33	3.12	.351 (ns)

Using SPSS 14.0, we computed the correlations between the constructs. As shown in Table 7, BI = Behavioral Intention; ATT = Attitude; SN = Subjective Norm; PBC = Perceived Behavioral Control; and TA = Technology Awareness.

TABLE 7: Correlation Matrix

	ATT	SN	PBC	TA
BI	.691**	.198	.408**	.409**
ATT		.310*	.432**	.485**
SN			.107	.312*
PBC				.617**

*p < .05; **p < .01

Based upon these results, we state the following regarding our hypotheses:

Hypothesis 1, Attitude is positively correlated with Behavioral Intention to use anti-spyware tools, is supported (r = .691; p < .01).

Hypothesis 2, Subjective Norm is positively correlated with Behavioral Intention to use anti-spyware tools, is *not* supported (r = .198; p > .05).

Hypothesis 3, Perceived Behavioral Control is positively correlated with Behavioral Intention to use anti-spyware tools, is supported (r = .408; p < .01).

Hypothesis 4, Technology Awareness is positively correlated with Behavioral Intention to use anti-spyware tools, is supported (r = .409; p < .01).

6. DISCUSSION

We were surprised to find a non-significant correlation between the Subjective Norm construct and Behavioral Intention. A number of previous studies using the Theory of Planned Behavior (TPB) have found a significant relationship between these two constructs. However, as expected, we found significant correlations between Attitude and Behavioral Intention and between Perceived Behavioral Control and Behavioral Intention.

We also found a significant correlation between the Technology Awareness construct and Behavioral Intention. Technology Awareness (r = .409) and Perceived Behavioral Control (r = .408) had almost identical correlations with Behavioral Intention. Future work should further explore the importance of Technology Awareness in this domain, as it seems to have similar importance as Perceived Behavioral Control. With a larger sample size, future research could use regression analysis or structural equation modeling to explore the importance of the Technology Awareness construct, as suggested in Figure 2.

Our findings suggest that students tend to learn about anti-spyware tools from personal experience, research, or through being taught by someone. We believe that interventions could be designed to target the influences relating to Attitude, Perceived Behavioral Control, and Technology Awareness.

The differences between CIS and non-CIS majors are possibly due to several reasons. CIS majors see their peers using anti-spyware software more than non-CIS ma-

jors. CIS majors also seem to have faster computers in which anti-spyware tools will not slow them down. This may be one of the reasons that some non-CIS majors do not intend to use anti-spyware software, as older computers do not run effectively with some tools.

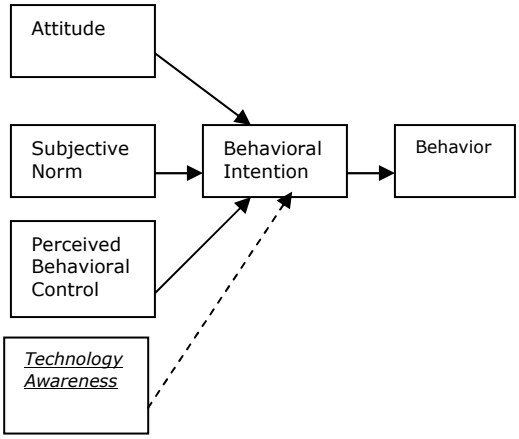

Figure 2: Proposed Addition to TPB

As shown earlier in Table 3, students majoring in CIS also have more resources, knowledge, and ability to run anti-spyware tools than non-CIS majors. Overall, CIS majors are more aware about the problems caused by spyware than non-CIS majors.

Through our findings at the walk-in center and through the survey and interviews we conducted, we believe we need to better educate and influence students, especially non-CIS majors, to use anti-spyware tools. It is important that we make sure that students are using these tools on a regular basis due to the facts that are represented in the introduction and spyware literature review section.

We believe spyware should be addressed in a class that every college student is required to take. None of the non-CIS majors indicated in their interviews that they have learned about spyware in their college classes. Teaching this material in a course designed for *all* college students (as opposed to only CIS majors) would hopefully result in them adopting anti-spyware tools voluntarily, which would lead to continued use throughout their lives. If students continue to use the anti-spyware tools, this will result in safer computer environments in colleges, homes, and businesses.

7. CONCLUSION

Our research identifies some of the factors influencing a student to adopt anti-spyware tools. The research needs to have a larger sample in order to be more conclusive, as our current sample size is not adequate to conduct higher-level statistical analysis. In future work, we plan to collect enough data to conduct a regression or structural equation modeling analysis using the Theory of Planned Behavior. With further research, we believe that we will find more evidence for the constructs that have already appeared to be important.

We believe that spyware is going to become more of a problem unless we find ways to persuade more college students to adopt the use of anti-spyware tools. Continued research will give us more insight into what influences college students, as well as others to adopt anti-spyware tools. With this knowledge, we will hopefully be able to find ways to reduce the spyware problem.

8. REFERENCES

Ajzen, I. (1991) "The Theory of Planned Behavior." Organizational Behavior and Human Decision Processes, 50,179-211.

Chenoweth, T., R. Minch, & T. Gattiker (2009) "Application of Protection Motivation Theory to Adoption of Protective Technologies." Proceedings of 42nd Hawaii International Conference on System Sciences.

Claburn, Thomas (Jan 21, 2009) "70 Of Top 100 Web Sites Spread Malware." InformationWeek. Retrieved February 9, 2009, from http://www.informationweek.com/news/internet/security/showArticle.jhtml?articleID=212901775.

"Consumer Reports Survey: U.S. Consumers Lost Nearly $8.5 Billion to Online Threats." (August 4, 2008). Retrieved February 9, 2009, from Academic OneFile.

Davis, F. (1989) "Perceived Usefulness, Perceived Ease of Use, and User Acceptance

of Information Technologies", MIS Quarterly 13(3), 319-340.

Davis, L.E., I. Ajzen, J. Saunders, and T. Williams (2002) "The decision of African American students to complete high school: An application of the theory of planned behavior". Journal of Educational Psychology, 94 (4), pp. 810-819.

Dinev, T. and Q. Hu (2007) "The Centrality of Awareness in the Formation of User Behavioral Intention toward Protective Information Technologies". Journal of the Association for Information Systems, 8(7), 386-408.

GovTrack.us. H.R. 1525—110th Congress (2007): Internet Spyware (I-SPY) Prevention Act of 2007, GovTrack.us (database of federal legislation) <http://www.govtrack.us/congress/bill.xpd?bill=h110-1525> (accessed Feb 09, 2009)

Internet Spyware (I-SPY) Prevention ACT of 2007, and the Securing Aircraft Cockpits Against Lasers Act of 2007. Hearing before the subcommittee on crime, terrorism, and homeland security of the committee on the judiciary house of representatives. Retrieved on February 9, 2009 from http://judiciary.house.gov.

Kumar, N., K. Mohan, and R. Holowczak (2008) "Locking the door but leaving the computer vulnerable: Factors inhibiting home users' adoption of software firewalls." Decision Support Systems 46(1) 254-264.

LaRose, R., N. Rifon, S. Liu, and D. Lee (2005) "Online Safety: A Content Analysis and Theoretical Assessment." Retrieved February 9, 2009, from https://www.msu.edu/~isafety/papers/icapanelca2.htm.

Lee, Y. and K. Kozar (2008) "An Empirical Investigation of Anti-spyware Software Adoption: A Multitheoretical Perspective." Information & Managment 45(2) 109-119.

Lee, Y. and K. Kozar (2005) "Investigating Factors Affecting Adoption of Anti-Spyware Systems." Communications of the ACM 48(8). 72-77.

Lee, Y., J. Lee, and Z. Lee (2006) "Social Influence on Technology Acceptance Behavior: Self-Identity Theory Perspective." ACM SIGMIS Database, 37(2 & 3), 60-75. Retrieved February 9, 2009, from The ACM Digital Library.

Rawstorne, P., R. Jayasuriya, and P. Caputi (2000) "Issues in Predicting and Explaining Usage Behaviors with the Technology Acceptance model and the Theory of Planned Behavior when Usage is Mandatory." ICIS '00: Proceedings of the Twenty-first International Conference on Information Systems, 35-44. Seltzer, Larry. AVG: Number of Malware Sites Spiking (Jan 27, 2009). PC Magazine Online, Retrieved February 9, 2009, from Academic OneFile.

Sipior, J. and B. Ward (March 2008) "Trust, privacy, and legal protection in the use of software with surreptitiously installed operations: An empirical evaluation." Information Systems Frontiers 10(1), 3-18.

Spyware. (2009). In Merriam-Webster Online Dictionary. http://www.merriam-webster.com/dictionary/spyware, Retrieved February 9, 2009.

Appendix

Structured Interview Questions

What is your major?

What year are you? (Sophomore, Junior, . . .)

Do you use anti-spyware tools?

What influenced you to use the specific anti-spyware tools that you use?

What type or brand of anti-spyware tools do you use?

How did you learn about spyware and the anti-spyware tools?

What has influenced your decision to use the anti-spyware tools? (ex. Friends, Family, Work, etc.)

Do you try to convince others to use the anti-spyware tools? If so, do they use them after you recommend them?

Concerning people who influence you that use anti-spyware tools: Does / did their influence and use of anti-spyware tools cause you to adopt the tools?

Do you believe that you have the resources to adopt anti-spyware tools?

Do you believe that you have the knowledge to adopt anti-spyware tools?

Do you believe that you have the ability to adopt anti-spyware tools?

By using anti-spyware tools do you believe that your computer is safer?

What is your attitude towards using anti-spyware tools?

Do you feel that using anti-spyware tools is an inconvenience or a hassle? Explain.

Do you have anything else you would like to share about your spyware experiences?