2005

# The Centrality of Awareness in the Formation of User Behavioral Intention Toward Preventive Technologies in the Context of Voluntary Use

Tamara Dinev
*Florida Atlantic University*, tdinev@fau.edu

Qing Hu
*Florida Atlantic University*, qhu@fau.edu

# The Centrality of Awareness in the Formation of User Behavioral Intention Toward Preventive Technologies in the Context of Voluntary Use

**Tamara Dinev**
Florida Atlantic University
tdinev@fau.edu

**Qing Hu**
Florida Atlantic University
qhu@fau.edu

**ABSTRACT**

Little is known about user behavior toward what we call preventive computer technologies that have become increasingly important in the networked economy and society to secure data and systems from viruses, unauthorized access, disruptions, spyware, and similar harmful technologies. We present the results of a study of user behavior toward preventive technologies based on the frameworks of theory of planned behavior in the context of anti-spyware technologies. We find that the user awareness of the issues and threats from harmful technologies is a strong predictor of user behavioral intention toward the use of preventive technologies. In the presence of awareness, the influence of subjective norm on individual behavioral intention is significantly weakened among less technology savvy users but strengthened among more technology savvy users. Also, commonly strong determinants "perceived ease of use" and "computer self-efficacy" in utilitarian technologies are no longer as significant in preventive technologies. Theoretical and practical implications are discussed.

**Keywords**

Awareness, Spyware, theory of planned behavior, preventive technology, behavioral intention.

## INTRODUCTION

The expansion of the computers and Internet presents great challenges to the evolving information society and the economy. Computer users have faced through the years many different threats to the security and well-being of their computers caused by technologies designed for negative impact on the systems, individuals, and corporations. The variety and complexity of cyber attacks, viruses, spam, and intrusions that have been developed parallel the variety and complexity of the information technologies that have been deployed, with no end in sight for either. As more and more security products are developed and coming onto the market, the developers of the "bad" technologies find ways to bypass these products and refine their software, which in turn leads to more refined security products. This cycle of reinforcing attack and deterrence continues with even greater intensity (Bagchi and Udo, 2003).

The innovation diffusion literature and technology acceptance models are usually concerned with innovations which aim to have a beneficial impact and thus the existing research is biased towards the "good" innovations. The study of innovations and technology which have negative impacts such as security attacks, viruses and spyware are scarce and just beginning to emerge (Bagchi and Udo, 2003, Stafford and Urbaczewski, 2004). As recognized by Stafford and Urbaczewski (2004), in the case of spyware little empirical work supports the many suppositions being made about spyware and its effects on personal and business computing. The reported attitudes are conflicting and not supported by solid scientific studies. Strong theoretical foundations and empirical validations are still lacking for considering users' behaviors in response to negatively affecting technologies such as spyware. Setting the research agenda on these issues, Stafford and Urbaczewski (2004) point that the only published research on the spyware problem in mid-2004 is what appears in law journals. Understanding end user attitudes and requirements is an essential step in this research process (Stafford and Urbaczewski, 2004).

The main research question of this study is: what are the factors that influence the user intentions and actions to use preventive technologies to eliminate harmful and malicious computer technologies? In answering the research question, we recognize the need to develop a more coherent theoretical foundation addressing individual Internet users' attitudes and behaviors in the practically policy-free Internet environment where the risk of disruption or damage brought by other malicious technologies such as spyware and computer viruses is high. This is in contrast to the well researched acceptance models concerning technologies that are either utilitarian or hedonic (Venkatesh et al., 2003; Van der Heijden, 2004), that is, technologies that bring positive and measurable benefits to users. To understand user attitude and behavior in this context, we introduce the construct of awareness, or more precisely for the case of technology usage, technology awareness based on the literature in sociology and other disciplines.

## RESEARCH MODEL

### Theory of Planned Behavior and Technology Acceptance Model

To understand the user behavior towards preventive technologies in the voluntary use environment, we draw on the theoretical bases of the theory of planned behavior (TPB) (Ajzen, 1988) and the research on technology acceptance of utilitarian technologies (Davis, 1989; Venkatesh et al., 2003). TPB contends that a person's behavior is determined by his or her intention to perform the behavior of interest. This behavioral intention is in turn determined by three factors: attitude towards the behavior (ATB), subjective norm (SN), and perceived behavioral control (PBC). PBC is an antecedent to both the intention and behavior (Ajzen, 1988).

Following Pavlou and Fygenson (2005), we introduce two additional constructs as underlying dimensions of 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 (Bandura, 1986), in our case, to clean spyware from their computers. And controllability is defined as the individual's judgments about the availability of resources and opportunities to perform the behavior (Pavlou and Fygenson, 2005).

In response to the limitations associated with TRA in predicting and explaining user acceptance of a new IT, Davis (Davis, 1989) developed TAM introducing two key factors that are important for user acceptance of a new IT: perceived ease of use (PEOU) and perceived usefulness (PU). PEOU is defined as the degree to which the user expects that usage requires limited effort. 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.

### Technology Awareness

The case of user response towards preventive technologies, such as anti-spyware software, has not been studied extensively mainly because the focus was technologies viewed as positively influencing job performance. Unlike IT usage in organizations and unlike voluntary e-commerce adoption, existence of spyware, viruses, and similar IT threats are often not known to the end user. Even less known are the strategies and tools needed to provide protection and elimination of the threats. Obviously, the case of fighting and eliminating negative IT resembles the case of fighting and eliminating medical diseases, social crimes and injustices, etc. In the case of voluntary use, therefore, the awareness, the raised consciousness and knowledge about a certain technology and its personal and social benefits and risks comes as a key factor in the process of voluntary IT usage.

Goodhue and Straub (1991) developed and tested a model that suggests that an individual's belief in the adequacy of security is a function of several factors among which awareness. The authors found weak and partial support of their hypotheses that awareness of the technology will have higher concern for security. As recognized by them, most probably the reason is that years of experience with information systems is a weak measure of security awareness injecting additional error and noise into their measurements. Nevertheless, the importance of this study far outweighs its deficiencies.

By examining the literature in social studies, criminal and medical behavioral science, we advance the definition and measurement of awareness and apply the concept to user behavior towards harmful information technologies. Awareness has been defined in the literature as the individuals' passive involvement and raised interest towards certain issues (Bickford and Reynolds, 2002, Green and Kamimura, 2003, Tillman, 2002). Following Dinev and Hart (2005) we adapt the term awareness to the technological issues and define *technology awareness* as the user's following and being interested in and knowledgeable about technological issues, problems and strategies to solve them.

We argue that the level of technological awareness will be a key factor influencing the attitudes and beliefs about the need to fight spyware and/or other computer threats. Indeed, the more a user is knowledgeable about the existing problems and consequences of cyber attacks and threats and ways to prevent them, the more he or she will form a positive attitude toward the need of eliminating these threats and protecting the systems from them. Since the use of anti-spyware technologies at individual level is more a choice than a mandate or necessity, an individual is unlikely to be motivate unless he or she is aware of the technology and the consequences of using or not using it. Thus, we propose:

*H1: Awareness positively influences user attitudes toward using anti-spyware technologies.*

In addition to attitude toward behavior, according to the theory of planned behavior, behavioral norms of the social group an individual user is closely associated with also have a strong influence on the behavioral intention of the individual (Ajzen, 1988). However, the behavioral norms of the social group about a phenomenon, such as spyware and anti-spyware technologies, are inevitably influenced by the members' awareness of the technologies and their consequences while shaping the behavioral intentions of individual members. The process of building awareness guides the development of a network of social organizations that begin to strongly advocate for policies and programs that are reducing the problem presence or use (Biglan and Taylor, 2000). In the case of spyware and security breaches which affect Internet users, the social networks and organizations will be formed by the parties interested in solving the spyware problem - Internet providers, software companies and computer makers which all are making efforts to increase awareness of the threats, as mentioned in the Introduction. Through building alliances and through extensive media usage, these networks' goal is, by increasing the awareness, to change the Internet users' group norms and build societal intolerance towards spyware and similar threats. It is reasonable to argue that the higher the degree of

awareness, the stronger the group norms. Thus, we propose:

*H2: Awareness positively influences the subjective norm about anti-spyware technologies.*

Given the fact that spyware could and often do inflict devastating damages to individuals and organizations, such as negative publicity, significant financial losses, and uncertain legal consequences, as they are often reported in the popular media, we argue that it is possible that awareness alone could motivate user to take action, regardless whether the user has formed a positive attitude or the social group norms. This argument is supported by other studies in medical literature and crime prevention where heightened awareness directly influences intention to helping behavior (Carlson et al., 1988).

*H3: Awareness positively influences user intention to use anti-spyware technologies.*

The relationships among other constructs, such as the one between "Perceived Usefulness (PU)" and "Attitude towards Behavior (ATB)" are well established in the literature of user technology acceptance research. However, for the completeness of this study, we include these hypotheses in our model. All are shown in our final research model as presented in Figure 1.

## RESEARCH METHODOLOGY AND DATA

The measurement for the TPB constructs - behavior (B), behavioral intention (I), attitudes toward behavior (AB), subjective norm (SN), and perceived behavioral control (PBC), ad well as the perceived usefulness (PU), perceived ease of use (PEOU), self-efficacy (SE), and controllability (C), were drawn from existing instruments in the literature (Bandura, 1986; Taylor and Todd, 1995; Koufaris, 2002; Pavlou and Fygenson, 2005, Venkatesh et al., 2003).

The development of the scales for the new awareness (A) construct was done by the authors. We examined awareness measurement instruments in other fields, such as sexual awareness scale (Snell and Wooldridge, 1998), family awareness scale (Kolevzon, 1985) in psychology; situational awareness in cognitive sciences (Durso and Gronlund, 2000) and medical sciences (disease prevention management Vega et al., 1998), and privacy-related IS research (Dinev and Hart, 2005). The existing social awareness instruments (Green and Kamimura, 2003; Dinev and Hart, 2005) provided an important guidance and base to build on. The instrument was then pilot tested for clarity, consistency, and validity with 87 students from the authors' programming classes. Scale purification and refinement followed. The pilot test resulted in only minor changes to the instrument.

A survey among IS professionals and students of a large Southeastern university was conducted to test the research model. Students enrolled in various classes were asked to fill in the online questionnaire in class time. Alternatively, students who did not have access to computers in their classes were asked to fill a paper survey. Additionally, an e-mail campaign with a request to participate in the study was initiated to IS professionals who graduated from this university with MIS/CS degrees. Links to the study's survey were posted on the web pages of the authors inviting the visitors to take the survey. A total number of 339 responses were received, out of which 7 were unusable because of many missing data items.

The research model was tested through Structural Equation Modeling (SEM) with LISREL. We used the two-stage approach to first assess the quality of our measures through CFA stage, and then test the hypotheses through the structural model, the SEM stage. The CFA stage was performed on the entire set of items simultaneously with each observed variable restricted to load on its a priori factor. All the necessary steps in the measurement model validation and reliability assessment were conducted following the widely used validation heuristics recommended for SEM by Byrne (1998) and Gefen et al. (2000).

The analysis resulted in a converged, proper solution with a low $\chi^2$ per degree of freedom and a good fit as indicated by all the listed fit indices. Collectively, the data from the model fit indices, factor loadings, and t-values suggest that the indicators account for a large portion of the variance of the corresponding latent construct and therefore provide support for the convergent validity of the measures (Gefen et al., 2000). The high values of the reliability coefficients provide further evidence of reliability of the scales. The structural model (Figure 1) shows the completely standardized parameter estimates between all latent variables. The results provided strong support for the majority of the hypotheses of the study, with most of the regression coefficients statistically significant at level .01.

## DISCUSSIONS, POST-HOC ANALYSIS, IMPLICATIONS

The empirical results from our study rendered support for most of the hypotheses with exception of H6, H10, and H13, where the hypothesized relationships were found to be not statistically significant. These hypotheses involve the subjective norm, perceived ease of use, and self-efficacy. Because the measurement instruments used for these constructs have been tested and validated in the current and previous studies, we have high degree of confidence in the adequate measurement of these constructs. Hence, we believe that there are theoretical reasons for the lack of statistical significances in the above relationships.

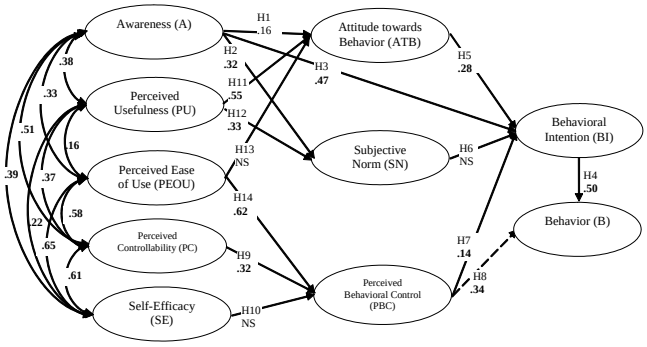


**Figure 1. Structural Equation Model with Parameter Estimates**

The insignificance between PEOU and ATB may be attributed to the phenomenon that a user feels forced to use preventing technology not because he or she likes it but because he or she perceives there is a real threat to the computer and/or the personal information being compromised. In that sense, the extent to which a user feels about a certain technology being easy to use will less likely affect his or her attitude towards using the prevention. A similar argument can be made about the diminished role of self-efficacy on the perceived behavior control (H10).

The lack of statistical significance between SN and BI is harder to explain without further analyzing the empirical data. For that purpose, we ran a model excluding the awareness construct reducing the model to the ones previously reported in the literature (Pavlou and Fygenson, 2005). The new model preserved the nature of all other relationships (including the lack of statistical significance between PEOU and ATB, and SE and PBC) except for SN-BI which now becomes statistically significant at level .01, with regression coefficient .19. Running the alternative model was important for two reasons. First, it reproduces and thus validates the empirical model with respect to the previously published models. Second, the change of SN-BI relationship confirms the importance of the direct relationship between awareness and behavioral intention. Without the awareness construct present in the model, SN takes over the influence of the missing awareness construct and thus renders statistically significant effect on BI.

To understand the nature of the SN-BI relationship better, we performed a multi-group analysis on two distinguishable groups that constitute our study: 161 respondents with MIS/CS degrees or majors (i.e. advanced IT users with more expertise in IT), and 163 respondents with other business degrees (i.e. not advanced IT users which use IT predominantly for word processing, email and WWW browsing). We believe that, although there is enough theoretical variance to support the model, the notion of belonging to a group in our case of broad sample of Internet users can be further refined. After validating the instrument items by establishing convergent and discriminant validity and reliability for each group, we proceeded to test the model separately for each group. Four of the path coefficients proved to be statistically different between the two groups, as established by $\chi^2$ difference test. The differences are given in Table 1.

| Relationship | IT Group | Non-IT Group | Full Sample |
|---|---|---|---|
| **SN-BI** | .25 | NS | NS |
| **PU-SN** | .16 | .48 | .33 |
| **A-BI** | .20 | .49 | .47 |
| **PBC-BI** | .26 | NS | .14 |

**Table 1. Path Coefficients For Each Group (All path coefficients are significant at level .01, except for NS (not significant)).**

It is immediately seen that the influence of subjective norm on behavioral intention is stronger for the IT savvy group than the non-IT group. We believe that the IT group is a more cohesive group in which individuals communicate more about IT related issues and are keen to learn what their peers are using to solve a problem than the non-IT group. Thus, the influence of peers on individual behavior tend be stronger in the IT group than in the non-IT group. In the IT group, the more aware they are, the more they will communicate and seek solutions within their social circle, exchange know-how and ideas. In contrast, awareness inspires acting but not communication in the non-IT group. There is no peer discussion about technology problems and thus the social circle does not exert influence on how an IT user will react to a problem. Thus the study reveals the most important problem of reaching these groups through establishing pro-active social networks and groups to educate and advocate about the necessity to prevent computer systems and individuals from harmful technologies.

The weaker influence of PU on SN for the IT group can also be explained by the characteristics of the two different groups. IT savvy individuals are more prone to experiment with a technology even if they don't perceive it s very useful. Thus suggestions to use or try a tool may influence the IT peers much more and much more easily than the non-IT users the latter needed to be convinced that the tool is indeed useful.

The weaker relationship between A and BI for the IT group can be attributed to the stronger SN influence on BI for that group. Indeed, because non-IT users do not communicate about technology as much as the IT-savvy users, being aware about a problem inspires them to act, while the member of the IT group would hear and weigh the peer's opinion and then act.

Finally, we should note that for the non-IT group, PBC does not have effect on behavioral intention. This may be related to the less experience the non-IT group has with information technologies. We suspect that individuals in the non-IT group practically felt little sense of control

when dealing with viruses or spyware threats and computer technologies in general.

In this paper, we presented the results of a study on the user behavior towards preventive technologies as opposed to the widely researched user acceptance of utilitarian technologies. We find that in the environment of voluntary use of preventive technologies, many of the previously established relationships of user technology acceptance behavior are no longer valid. More importantly, awareness becomes the central determinant of user attitude and behavior towards the technology. Our findings have both significant theoretical and practical implications. Theoretically, we introduced the awareness construct into technology acceptance research. Practically, our findings provide some insights for mangers to design more effective security policies and practices in conjunction with technologies in the fight against the onslaught of spyware and other Internet-spawn malware technologies. For example, our findings call for awareness as the center piece of any effective information security policies. We also argue that to reach the average home Internet users, because these users do not belong to a more cohesive social circle as far as IT usage is concerned, the traditional information channels – media, television and newspapers should play an important role in forming a social pressure and policies that address information security issues in the globally connected society and economy.

## REFERENCES


Ajzen, I. Attitudes, Personality, and Behavior. (1988) The Dorsey Press, Chicago, IL 60604.

Bagchi, K. and Udo, G. (2003) An Analysis of the Growth of Computer and Internet Security Breaches, Communications of the Association for Information Systems, 684-700.

Bandura, Albert. (1986). *Social foundations of thought and action: A social cognitive.* Englewood Cliffs, NJ: Prentice Hall.

Biglan, A. and Taylor, T.K. (2000). "Why Have We Been More Successful in Reducing Tobacco Use Than Violent Crime?", *American Journal of Community Psychology*, 28, 3, 269 – 302.

Bickford, D. M. & Reynolds, N. (2002) Activism and service-learning: reframing volunteerism as acts of dissent. Pedagogy, *Critical Approaches to Teaching Literature, Language, Composition and Culture*, 8, 2, 229-252.

Byrne, B. (1998) *Structural Equation Modeling with LISREL, PRELIS, and SIMPLIS*. Lawrence Erlbaum Ass., N.J.

Carlson M, Charlin V, Miller N. J. (1988) Positive mood and helping behavior: a test of six hypotheses, *Perspectives of Social Psychology,* 55, 2, 211-29.

Davis, F. D.: "Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology" *MIS Quarterly*, 1989, 13, 319-340.

Dinev, T. and Hart, P. (2005). Internet privacy concerns and social awareness as determinants of intention to transact, International Journal of E-Commerce, forthcoming.

Durso, F. & Gronlund, S. (2000). Situation Awareness, in F. Durso et. al. (eds.) *Handbook of Applied Cognition*., 283-314, NY: Wiley.

Gefen, D., Straub, D. W., Boudreau, M.C. (2000). Structural Equation Modeling And Regression: Guidelines For Research Practice, C*ommunications of AIS*, 4, Article 7.

Goodhue, D.L. and Straub, D.W. (1991). "Security concerns of system users: A study of perceptions of the adequacy of security", *Information & Management* 20, 13-27.

Green, S. P., Kamimura, M. (2003). Ties that bind: enhanced social awareness development through interactions with diverse peers, *Annual Meeting of the Association for the Study of Higher Education*, Portland, Oregon.

Karahanna, E., Straub, D. W., & 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.

Kolevzon MS; Green RG. (1987) Family awareness scales [FAS], IN: Corcoran K & Fischer J. Measures for clinical practice: A sourcebook. New York: Free Pr., 436-439.

Koufaris, M. (2002) Applying the Technology Acceptance Model and Flow Theory to Online Consumer Behavior, *Information Systems Research* (13:2), 205-223.

Pavlou, P. A. and M. Fygenson (2005). Understanding and Predicting Electronic Commerce Adoption: An Extension of the Theory of Planned Behavior," *MIS Quarterly (forthcoming)*.

Snell, W. E., Jr., & Wooldridge, D. G. (1998). Sexual awareness: Contraception, sexual behaviors and sexual attitudes. Sexual and Marital Therapy, 13, 191-199.

Stafford, T. F. and Urbaczewski, A. (2004) Spyware: The Ghost In The Machine, *Communications of the Association for Information Systems*, Volume14, 291-306.

Taylor, S. and Todd P.A. (1995). Understanding Information Technology Usage: A Test of Competing Models, *Information Systems Research*, 6, 3, 144-176.

Van der Heijden, H. (2004) User Acceptance of Hedonic Information Systems. *MIS Quarterly*, 28, 4, 695-704.

Venkatesh, V., Morris, M. G., Davis, G. B., and Davis, F. D. (2003) User Acceptance of Information Technology: Toward a Unified View. MIS Quarterly, 27, 3.