PACIS 2005 Proceedings

Pacific Asia Conference on Information Systems (PACIS)

December 2005

A Socio-Behavioral Study of Home Computer Users' Intention to Practice Security

Boon-Yuen Ng
National University of Singapore

Mohammad Rahim
National University of Singapore

A Socio-Behavioral Study of Home Computer Users' Intention to Practice Security

Ng, Boon Yuen
Department of Information Systems
National University of Singapore
ngby@comp.nus.edu.sg

Rahim, Mohammad Azree
Department of Information Systems
National University of Singapore
mdazree_seville@yahoo.com

Abstract

Home computer users play a crucial role in securing the cyberspace, but the protection of home computers is left to the initiative of the users. In this study, we focus on the socio-behavioral perspective, as the behavior of home computer users on security issues is one of the most important factors in securing the cyberspace. The decomposed Theory of Planned Behavior is adapted to investigate the factors that influence a user's intention to practice home computer security. A survey instrument was developed and administered to 233 home computer users. The findings revealed that attitude and subjective norm determined intention to practice computer security, and perceived usefulness, family and peer influence, mass media influence and self-efficacy are important factors that influence a home computer user's intention to practice computer security. Findings also provide an impetus for researchers to conduct future studies in this domain.

Keywords: Computer security, End-user computing, Theory of Planned Behavior, Mass media

1. Introduction

In today's highly interconnected world, cybersecurity is a serious issue that requires attention. With 888 million Internet users (Internet Usage Statistics 2005), it is imperative to study the security of home computers connected to the Internet, as it has a direct impact not just on individual computers, but the security of the cyberspace, including critical infrastructures and services (such as telecommunication and banking) that are heavily dependent on the secure functioning of the cyberspace. Undefended home computers can become part of networks of remotely controlled machines that are then used to attack critical infrastructures (Department of Homeland Security 2003). Thus, we consider the practice of home computer security as a socially and personally positive behavior as it protects one's home computer and contributes to the security of the cyberspace.

While the security of computer systems in an organizational setting is governed by the organization's security policies, the protection of home computers is left to the initiative of the users. Therefore, the behavior of home computer users on computer security issues is probably one of the most important factors in determining whether these systems are sufficiently secured. Unfortunately, home computer users are generally unprepared to defend against attacks from the Internet (Carpenter et al. 2001). One of the biggest threats to home computer security is virus infection, which has the potential to threaten the confidentiality and integrity of information on computers as well as the availability of computers and networks. The damage is not limited to just home users, as the security of the cyberspace is affected. It is estimated that personal computer viruses cost businesses approximately $55 billion in damages in 2003 (Securitystats.com 2004).

The problems of computer security can, to a certain extent, be mitigated by technology-based solutions such as cryptography and authentication mechanisms. However, computer security is not just a technical issue. The success of security also depends on the effective behavior of users (Stanton et al. 2003). The human factor has repeatedly been said to be the weakest link in computer security (Economist.com 2002). It is thus necessary to study the socio-behavioral perspective and explore the factors that influence a user's intention to practice home computer security. A broader vision that addresses social groups and behavior is needed (Dhillon and Backhouse 2001). The impetus for our study is the fact that very little has been done to investigate the behavioral aspects of home computer users, with respect to computer security.

Our research question is, "What are the factors that will influence a home computer user's intention to practice computer security?" Through this study, we aim to contribute to the better understanding of human behavior in the context of home computing, so that effective strategies in spreading the computer security message to home users can be devised.

2. Literature Review

The framework used for this study is the Theory of Planned Behavior (TPB), a well-regarded and well-researched social cognitive model to explain human behavior.

2.1 Theory of Planned Behavior (TPB)

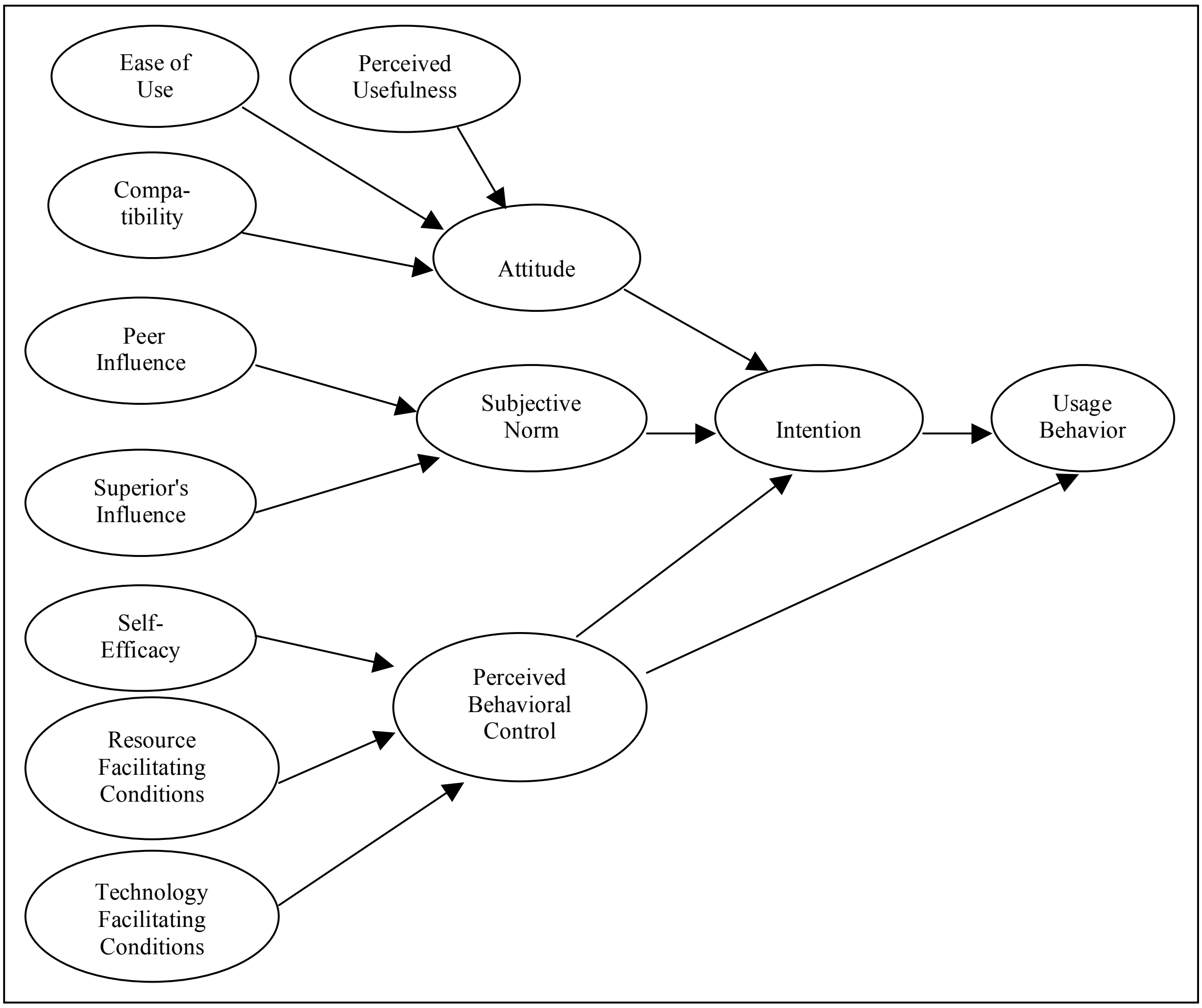
The TPB views a person's intention to perform a behavior as the immediate determinant of the action (Ajzen 1988). As a general rule, the stronger the intention to engage in a particular behavior, the more likely should be its performance (Ajzen 1991). The TPB states that intentions are determined by three factors – attitude towards the behavior, subjective norm, and perceived behavioral control (Ajzen 1988).

The validity of the TPB model has been verified empirically in psychology literature (Ajzen 1991; Ajzen and Madden 1986) and marketing literature (Taylor and Todd 1995b). TPB has been a good predictor of behaviors such as taking vitamins (Madden et al. 1992) and weight loss (Bagozzi and Kimmel 1995). The theory has also been successfully applied in several studies on general ecological behavior (Kaiser et al. 1999) and household recycling (Boldero 1995; Taylor and Todd 1995b). The predictive power of TPB's variables has also been validated in studies investigating Internet abuse (Galletta and Polak 2003) and e-commerce adoption (Paviou and Fygenson 2004). We consider the practice of home computer security as a socially and personally positive behavior as it protects one's home computer and contributes to the security of the cyberspace. Hence, it is appropriate to study this behavior by using the TPB.

2.2 Decomposed Theory of Planned Behavior

To better explain the relationship between behavior and intention, the TPB has been decomposed, modified and extended with new constructs by several authors (Chau and Hu 2001). In a research studying information technology use, two variations of the TPB along with the Technology Acceptance Model were tested (Taylor and Todd 1995a). Of the three, the decomposed TPB (Figure 1) provided a moderate increase in the explanation of intention. This is the model that we are adapting for this study, as it provides a better understanding of behavioral intention by focusing on factors that are likely to influence the user. Our research is thus consistent with IT usage studies with similar objectives, focusing on attitude, social influence and facilitating conditions (Hartwick and Barki 1994; Mathieson 1991).

Figure 1 - Decomposed Theory of Planned Behavior (Taylor and Todd 1995a)



In the original study, the researchers studied individuals' usage of an IT resource centre in an organizational setting (Taylor and Todd 1995a). To suit the context of our study, the constructs *Compatibility, Ease of Use*, *Technology Facilitating Conditions* and *Superior's Influence* are not included. Thus, the factors that we have retained for our project are those which we consider applicable to the home setting. For example, the construct *Superior's Influence* (Taylor and Todd 1995a) will not be studied as we are targeting home computer users and not employees in an organization. We will study *Family and Peer Influence* instead of just *Peer Influence*. This is because in studying of home computer users, family members' role in promoting pro-security behavior cannot be ignored. Besides studying the effects of people known to users (i.e. family members and peers), we are also interested in studying the effects of "unknown others", in the form of mass media.

2.3 Mass Media Influence

The subjective norm of mass media was first introduced and tested in the Ajzen's (1985) planned behavior model. The results indicated that people perceived influence from significant others as well as "unknown others" through the mass media. This illustrates the informal contribution of mass media to the learning and adoption of established norms, values and expectations of behaviors in given social roles and situations (McQuail 1987).

There is increasing evidence that the mass media serve as important sources of information for a wide range of topics (Dominick 1996). Mass media campaigns may be useful for raising an issue for public attention, such as drunk driving, or for introducing new concepts, such as what comprises a standard drink (Agostinelli and Grube 2002). Thus, besides acting as powerful means of information dissemination, mass media can also be used to promote activities that will benefit society.

There is little doubt on the role of the mass media as agents of socialization (Dominick 1996). One of the effects of this socialization process could be a behavioral change on the part of the receiver. In a study of the use of mass media to promote healthy eating, findings show that a media-only approach was sufficient to encourage a significant proportion of the people in one community to alter the dietary habit targeted by the intervention (Reger et al. 1999). In a TPB study investigating waste recycling behavior, mass communication stood out as one of the major sources of influence in the establishment of subjective norm (Chan 1998). This provides evidence on the merits of using the mass media to promote socially and personally positive behavior. In another study on e-commerce, external influence (which included mass media) was found to be an important predictor of subjective norm (Bhattacherjee 2000).

2.4 Practicing Computer Security

To practice computer security is to apply a set of recommended practices that would facilitate the achievement of the three common information security objectives – confidentiality, integrity and resource availability of computer systems (OECD 2002).

From our literature survey, there is a lack of credible academic sources that agreed on a common set of recommended practices, in relation to the security of home computer systems. Hence, we selected the practices based on recommendations for home computer users issued by the United States Computer Emergency Response Team Coordination Centre, the coordinating authority and source of information for all national computer emergency response teams worldwide (Rogers 2002). We studied three of the recommended practices to represent the practice of computer security. This is similar to the approach adopted by Ajzen and Driver (1992) who studied a set of five leisure activities as a representation of an individual's overall intention to engage in recreation. We chose practices that are representative of home computer security, easy to measure, independent of operating systems, and recommended by established vendors. Field experts were also consulted to refine the definitions of these practices. Hence, for this study, we investigated whether home computer users intend to:

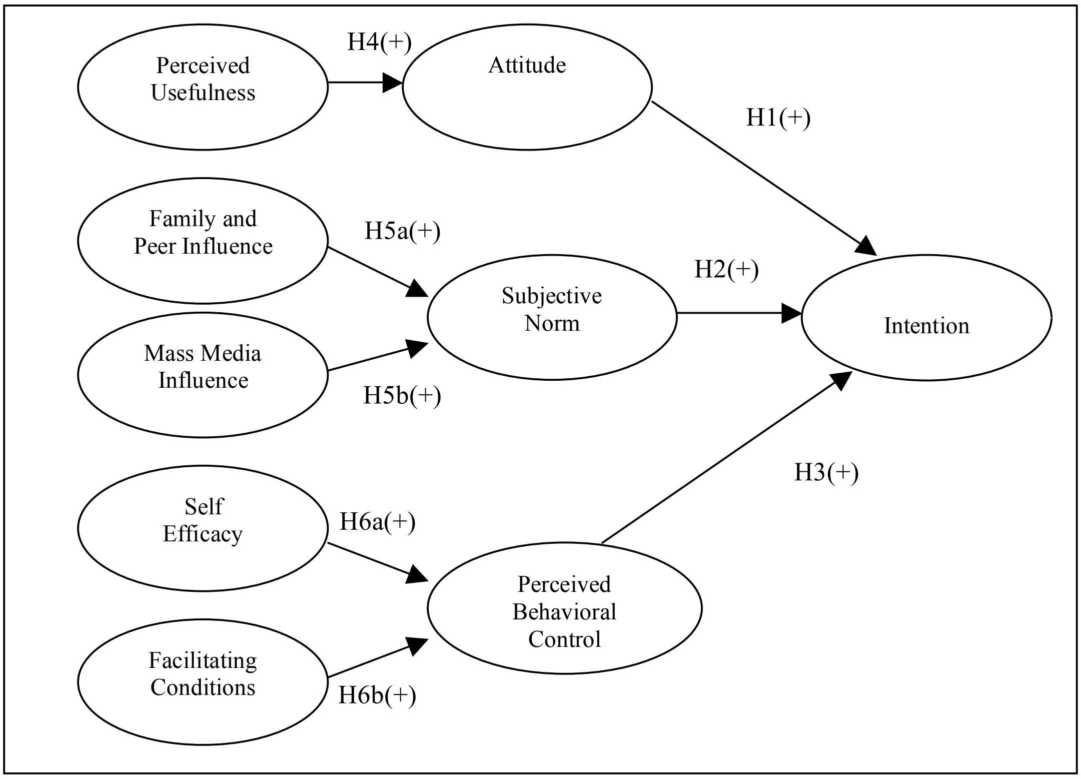
1) Update their anti-virus software regularly – This is important as virus infection is one of the biggest threats faced by home computer users. This is also a relatively easy task for users to perform.
2) Back up their critical data – This is vital in the event when integrity of the data residing in the computer is compromised by threat agents such as a virus or a hacker.
3) Use a personal firewall – A personal firewall monitors a personal computer’s connection to the Internet. Not only does it protect the computer, it also restricts outgoing traffic and indirectly contributes to the security of the cyberspace. The use of a personal firewall is more complex compared to other well-known protection measures such as anti-virus software.

3. Research Model

Figure 2 presents our research model, which is based on the decomposed TPB.

Results from a number of research studies have validated the role of intention as a proximal determinant of behavior (Ajzen 1988). These studies show that when an individual has the intention to perform a behavior that is within his volitional control, then it is likely that he will do so. In view of this, we did not study actual behavior for this study but focus on measuring intention.

Figure 2 – Factors influencing a home user's intention to practice computer security



We define each construct and present the related hypotheses below.

Intention **(INT)** – This refers to a home computer user's intention to practice computer security.

Attitude **(ATT)** – This refers to a home computer user's disposition (i.e. inclination or tendency) to respond favorably or unfavorably towards practicing computer security. We hypothesize:

> *H1: There is a positive relationship between a home computer user's attitude towards practicing computer security and his intention in practicing computer security.*

Subjective Norm **(SN)** – This refers to a person's perception of the social pressure to perform or not to perform the behavior under consideration, in this case, to practice computer security in home computers. This leads us to our second hypothesis:

> *H2: There is a positive relationship between subjective norm to practice computer security and a home computer user's intention in practicing computer security.*

Perceived Behavioral Control **(PBC)** – Perceived behavioral control is the person's perception of the extent to which performing a behavior is under his/her control (Sheeran et al. 2003). For our study, this refers to the home computer user's perception of control over his/her ability to practice computer security. This brings us to our third hypothesis:

> *H3: There is a positive relationship between a home computer user's perceived behavioral control and his intention in practicing computer security.*

Perceived Usefulness **(PU)** – Davis (1989) defines perceived usefulness as "the degree to which a person believes that using a particular system would enhance his job performance". In this study, we define perceived usefulness as the degree to which a home computer user believes performing a particular practice will enhance the security of his computer. Our fourth hypothesis is:

> *H4: There is a positive relationship between a home computer user's perceived usefulness of a security practice and his attitude towards performing that practice.*

Family and Peer Influence **(FPI)** – We define this as the influence or pressure from sources known to the home computer user (in this case, family and peers) to practice computer security. We hypothesize that:

> *H5a: There is a positive relationship between family & peer influence and subjective norm to practice computer security.*

Mass Media Influence **(MI)** – For this study, mass media is defined as mediums of communication such as newspapers, radio, television, Internet, broadcast e-mails, official announcements made by authorities, etc. that are designed to reach the mass of the people (The Oxford World Encyclopedia 2001). Mass media influence is defined as the influence or pressure from the mass media to practice computer security. The next hypothesis is:

> *H5b: There is a positive relationship between mass media influence and subjective norm to practice computer security.*

Self-Efficacy **(SE)** – Self-efficacy is an individual's self-confidence in his ability to perform a behavior (Bandura 1977). Self-efficacy affects perceived behavioral control as it is an internal factor that may impede performance of the behavior (Ajzen 1985, 1991; Ajzen and Driver 1992; Ajzen and Madden 1986). For this study, self-efficacy refers to a home computer user's self-confidence in his/her skills or ability in practicing computer security. The next hypothesis is:

> *H6a: There is a positive relationship between a home computer user's self-efficacy and his perceived behavioral control in practicing computer security.*

Facilitating Conditions **(FC)** – While self-efficacy measures the internal factor, facilitating conditions measures the external factor that may impede performance of the behavior. Taylor and Todd (1995a) define facilitating conditions as "the beliefs about the availability of resources to facilitate behavior". Here, we define this construct as a home computer user's beliefs about the availability of resources to facilitate him/her to practice computer security. For this study, we will investigate time and financial resources as facilitating conditions with the following hypothesis:

> *H6b: There is a positive relationship between facilitating conditions and a home computer user's perceived behavioral control in practicing computer security.*

4. Research Methodology

Our proposed research model is tested empirically with data collected through a survey instrument. As a number of items used for our survey have been adapted from their original sources to suit the context of our study, their validity must be systematically ensured.

4.1 Instrumentation

A survey instrument is developed following procedures recommended by Churchill (1979). We included the sorting procedure for the conceptual validation of instruments (Moore and Benbasat 1991).

We have a total of 25 items to measure the nine constructs in our model. The items were adapted from past validated items and measured using a seven-point Likert scale. The same set of items for each construct was used to investigate each individual computer security practice. This gives us a total of 75 items for the actual questionnaire. Items used to measure the constructs for the practice of updating anti-virus software are listed in Table 1.

Table 1 – Construct and Items (Updating Anti-Virus Software)

Construct	Items
Intention	▪ INT1: I intend to update my anti-virus software regularly within the forthcoming month. *(agree-disagree)* ▪ INT2: My intention to update my anti-virus software regularly within the forthcoming month is *strong-weak*.
Attitude	▪ ATT1: Updating my anti-virus software regularly within the forthcoming month would be *wise-foolish*. ▪ ATT2: Updating my anti-virus software regularly within the forthcoming month would be *beneficial-harmful*. ▪ ATT3: Updating my anti-virus software regularly within the forthcoming month would be *good-bad*. ▪ ATT4: Updating my anti-virus software regularly within the forthcoming month would be *enjoyable-unenjoyable*. ▪ ATT5: Updating my anti-virus software regularly within the forthcoming month would be *pleasant-unpleasant*.
Subjective Norm	▪ SN1: People and other sources that are important to me would recommend that I update my anti-virus software regularly within the forthcoming month. *(agree-disagree)*. ▪ SN2: People and other sources that influence my behavior would recommend that I update my anti-virus software regularly within the forthcoming month. *(agree-disagree)*
Perceived Behavioral Control	▪ PBC1: I have complete control over whether I update my anti-virus software regularly within the forthcoming month. *(agree-disagree)* ▪ PBC2: It is mostly up to me whether I update my anti-virus software regularly within the forthcoming month. *(agree-disagree)*
Perceived Usefulness	▪ PU1: I find updating my anti-virus software regularly within the forthcoming month useful in securing my computer and preventing virus attacks. *(agree-disagree)* ▪ PU2: I find updating my anti-virus software regularly within the forthcoming month effective in securing my computer and preventing virus attacks. *(agree-disagree)*
Family and Peer Influence	▪ FPI1: My family members would *approve/disapprove* of me updating my anti-virus software regularly within the forthcoming month. ▪ FPI2: My family members *expect/do not expect* me to update my anti-virus software regularly within the forthcoming month. ▪ FPI3: My peers would *approve/disapprove* of me updating my anti-virus software regularly within the forthcoming month. ▪ FPI4: My peers *expect/do not expect* me to update my anti-virus software regularly within the forthcoming month.
Mass Media Influence	▪ MI1: The mass media suggest that I should update my anti-virus software regularly within the forthcoming month. *(agree-disagree)* ▪ MI2: Mass media reports influence me to update my anti-virus software regularly within the forthcoming month. *(agree-disagree)* ▪ MI3: I feel under pressure from the mass media to update my anti-virus software regularly within the forthcoming month. *(agree-disagree)*
Self-Efficacy	▪ SE1: I would feel comfortable updating my anti-virus software on my own. *(agree-disagree)* ▪ SE2: I would be able to update my anti-virus software reasonably well on my own. *(agree-disagree)* ▪ SE3: I would be able to update my anti-virus software even if there was no one around to help me. *(agree-disagree)*
Facilitating Conditions	▪ FC1: I have the time to update my anti-virus software regularly within the forthcoming month. *(agree-disagree)* ▪ FC2: I have the financial resources to update my anti-virus software regularly within the forthcoming month. *(agree-disagree)*

The instrument validation process was carried out in two stages. First, pretest interviews were carried out to seek the assessment of academic and field experts on the clarity and correctness of our items. In the second stage, the sorting procedure consisting of two rounds was carried out (Moore and Benbasat 1991). To assess the sorting results, we calculated the Cohen's

Kappa (Cohen 1960) and item placement ratio (Moore and Benbasat 1991) values based on data collected from the judges' sorting. For both rounds, Cohen's Kappa and the average item placement ratio were greater than 0.92. As Kappa scores greater than 0.65 are deemed to be acceptable (Moore and Benbasat, 1991), the results show that the scales have high reliability.

4.2 Data Collection

The survey was administered to 233 undergraduates who are home computer users. The age group of undergraduates makes them particularly suitable for this study, as personal computer penetration and internet access are generally higher for younger people (OECD 2001) and undergraduates are generally IT-literate. The demographic profile is shown in Table 2.

Table 2 – Demographic Profile

Demographic Profile (Total respondents = 233)		
Sex	**Number**	**Percentage**
Male	145	62.2%
Female	88	37.8%
Age	**Number**	**Percentage**
19-24	222	95.3%
25-29	11	4.7%
Familiarity with Computer Security Practices	***Mean**	**Std. Deviation**
Updating anti-virus software	6.2489	0.9321
Backing up critical data	5.9914	1.1025
Using personal firewall	5.6223	1.2676

* A seven-point Likert scale was used. A higher score indicates a higher level of familiarity.

4.3 Data Analysis

We used Partial Least Squares to conduct our analysis. We assessed the model for each of the three practices and conducted tests of measurement and structural models. The measurement model looks at the loadings of observed items (measurements) on their expected latent variables (constructs), while the structural model looks at the assumed causation among a set of dependent and independent constructs (Gefen et al. 2000).

For our study, the constructs PU, SN, SE, PBC and INT are classified as reflective while ATT, FPI, MI and FC are considered formative. For the reflective constructs, internal consistency is measured by the Cronbach's alpha reliability coefficient (Cronbach 1951). Reliabilities of 0.50 to 0.60 would suffice (Nunnally 1978) and a score of 0.70 is recommended (Moore and Benbasat 1991). In analyzing the practices, we found the Cronbach's alpha for all the constructs to be higher than the recommended 0.70.

Convergent validity of the reflective constructs is assessed using three tests: (1) item reliability (2) composite reliability and (3) average variance extracted (AVE) per construct. For item reliability, each standardized item loading should be greater than 0.707 in order for the shared variance between each item and its intended construct to exceed the error variance (Chin 1998). All items fulfill this requirement. For the second test, the composite reliabilities of all the constructs are greater than the recommended 0.7 (Fornell and Larcker 1981). For the third test, AVE for all the indicators are greater than the required 0.50 (Fornell and Larcker 1981). Thus, our results show that all reflective constructs exhibit adequate levels of convergent validity.

We assessed the discriminant validity for reflective constructs by examining: (1) item loadings and (2) item correlations. Factor analysis using principal components analysis with a varimax rotation was executed for the first test of discriminant validity. In order to test the appropriateness of factor analysis, the Kaiser-Meyer-Olkin (KMO) measure of sampling adequacy was calculated. Out of the three practices, "Using personal firewall" yielded a KMO value 0.819 which can be characterized as meritorious. "Updating anti-virus" and "Backing up critical data" showed KMO values of 0.7 and 0.764 respectively, which is in the satisfactory "middling" category (Kaiser 1974). Five factors were extracted for the respective practices. For all the practices, the factors explained more than 80% of total cumulative variance. Factor loadings of all items on their intended construct are greater than the commonly accepted threshold of 0.5 (Hair et al. 1998). All factors have an eigenvalue greater than one. This indicates that the factors are stable and that the items anchor well onto the factor (Johnson and Wichern 1998). For the second test of discriminant validity, correlations between the measures of two constructs were examined. Results show that more variance is shared between the construct and its indicators than with another construct representing a different set of indicators (Chin 1998). This indicates adequate discriminant validity.

Thus, results show that all reflective constructs exhibit adequate levels of internal consistency, convergent validity and discriminant validity. For formative constructs, all item measures can be independent of one another, and absolute values of item weights are examined to determine the relative contribution of items constituting the construct (Chin and Gopal 1995). The item weights are shown in Table 3.

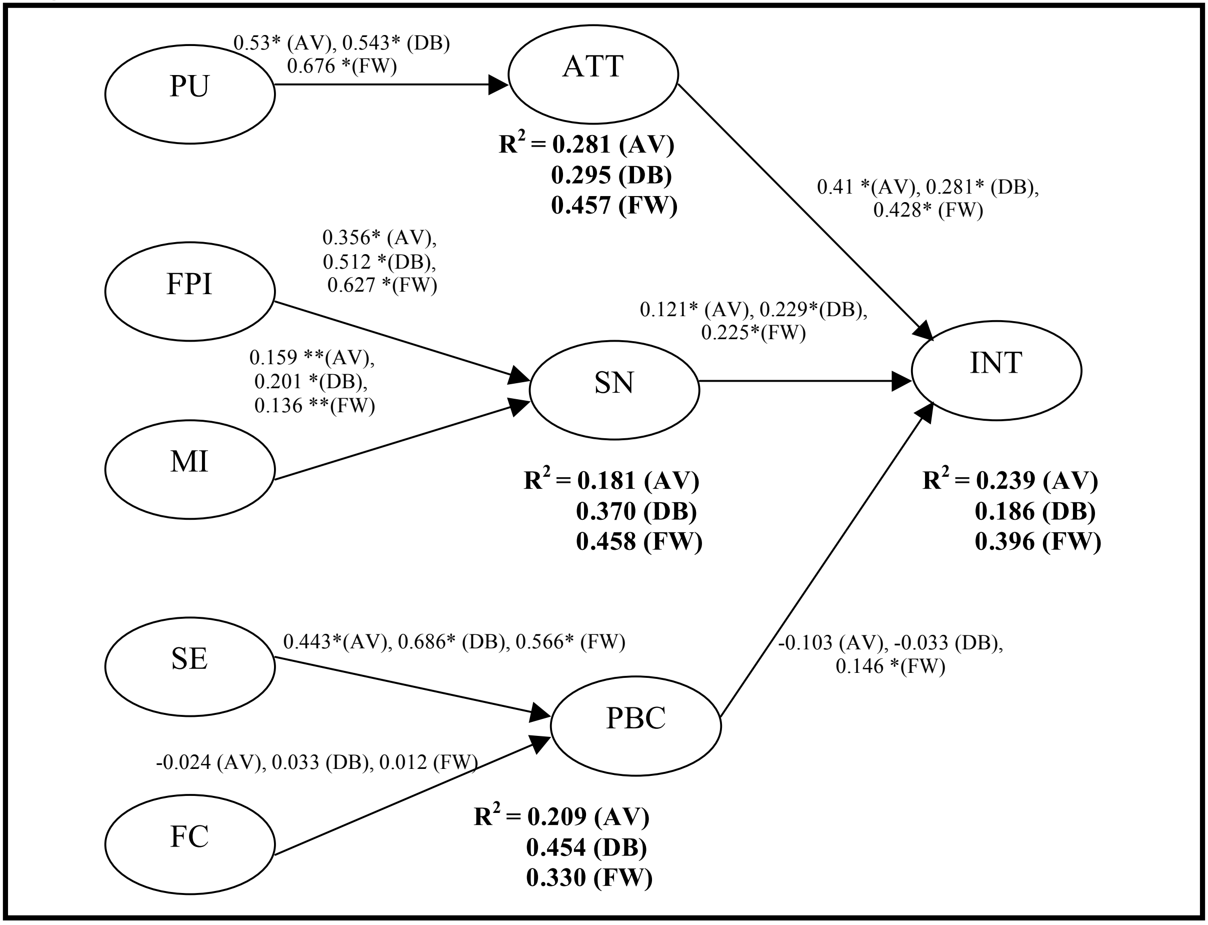
Table 3 – Item Weights of Formative Constructs

Construct	Item	Item Weights*		
		Antivirus	Data Backup	Firewall
Attitude	ATT1	0.3376	0.3507	0.3103
	ATT2	0.3243	0.3210	0.2948
	ATT3	0.3113	0.3062	0.2832
	ATT4	0.1526	0.1092	0.1394
	ATT5	0.1856	0.2384	0.1566
Family & Peer Influence	FPI1	0.2730	0.3707	0.2715
	FPI2	0.2166	0.2608	0.2076
	FPI3	0.3495	0.3037	0.3986
	FPI4	0.5474	0.4009	0.3732
Mass Media Influence	MI1	0.6130	0.7203	0.2962
	MI2	0.3565	0.4258	0.4504
	MI3	0.2649	0.0058	0.3579
Facilitating Conditions	FC1	0.6660	0.5000	0.6323
	FC2	0.5192	0.6786	0.5254

*All items are significant at the $p < 0.05$ level

To test the structural model, we used Partial Least Squares to assess statistical significance of the loadings (R^2) and path coefficients. The path coefficients and R^2 values for the individual models are displayed in Figure 3. For R^2, 10% is an indication of substantive explanatory power (Falk and Miller 1992). All R^2 values fulfilled this requirement. Thus, we consider that our model possesses a satisfactory level of predictive validity. Our model satisfies the criteria of a good model fit, as evident from the results of our measurement model and structural model evaluation.

Figure 3 – Test of Structural Model



* Significant at p< 0.01 Level , ** Significant at p<0.05 Level, AV=antivirus, DB=data backup FW=firewall

5. Discussion and Implications

For all three practices, we have found that attitude and subjective norm have a significant positive relationship with intention (H1 and H2). This is consistent with the TPB literature which posits the role of attitude and subjective norm as determinants of intention. However, the relationship between perceived behavioral control and intention (H3) is significant only for the practice of using a personal firewall. This suggests that the practice of updating anti-virus software and backing up critical data may be tasks over which home computer users have a high degree of volitional control. Hence, perceived behavioral control is not a significant factor in determining the intention to practice such behavior. Another possible contributing factor is the fact that a number of anti-virus software provide an automatic update feature. Such results are consistent with prior research where perceived behavioral control was found to have a non-significant effect on intention (Riemenschneider et al. 2002; Hagger et al. 2001). However, users may regard the use of a personal firewall to be more complex as personal firewall is a relatively new product, and thus perceived behavioral control is a significant factor. This is evident from Table 2 which indicates that the familiarity of respondents is the lowest for the practice of using a personal firewall.

Consistent with past studies, perceived usefulness was found to be a significant predictor of attitude (H4) for all three tasks (Davis 1989). This suggests that the usefulness of computer security practices should be stressed as they do influence users' attitude towards practicing security.

We also found family, peer and mass media influences to be significant antecedents of subjective norm (H5a and H5b). Items weights show that peer influence contributed more to subjective norm than family influence. As such, we should always remind those around us on the importance of protecting and securing our computer systems. This can be done through sharing knowledge and advice on such matters. The "security culture" should be promoted to all computer users. This is important as we are indirectly contributing to a safer Internet environment by securing our home computers. Mass media also plays a crucial role in promoting computer security. Mass media as a channel to educate home users on computer security practices should be fully utilized.

From our results, we have also verified the significant relationship between self-efficacy and perceived behavioral control (H6a). Therefore, it is necessary to equip home computer users with the necessary skills to use such technical solutions. However, our hypothesis that facilitating conditions relates positively to perceived behavioral control (H6b) was not supported. This may indicate that a person's ability to perform these security practices is influenced more by his individual ability than external factors such as time and financial resources. Another possibility is that facilitating conditions relates directly to behavior rather than perceived behavioral control (Triandis 1977).

6. Limitations and Future Research

Our study is limited to the three selected practices. As our comparison of the three practices show that factors affecting a user's intention to practice computer security differ in some ways, we suggest that future studies focus on individual practices in detail, as well as other recommended practices for home computer users.

Our study established the importance of mass media, but we did not study the individual forms of mass media, such as newspapers, television and Internet. The influence of different forms of mass media with regards to promoting good security practices may be different. We propose that future research should study the influence of specific forms of mass media and compare the results. This will help identify the form of mass media that is most suitable and effective in conveying the message of computer security.

Besides family, peer and mass media influences, there could be other factors that play a significant role in a home user’s intention to practice security. Future studies could explore other possible factors such as education and the role of the government.

The empirical results for our model provide support for the use of the decomposed TPB as a possible framework to study a home user's intention in practicing computer security. However, the unsupported hypotheses also suggest the plausibility of including other factors to this model. Exploratory and empirical tests can be performed to identify and explore the relationships in further detail. Future research should also aim to retain and enhance the predictive power of the proposed model and eliminate unnecessary variables that compromise its parsimony.

7. Conclusion

The solution to the computer security problem involves the combination of both technological and human factors. Through this study, we have examined the socio-behavioral perspective of computer security in the context of home computer users and established factors that are significant to the home users’ intention to practice home computer security.

This study has provided explanations and useful insights to the behavior of home computer users. Home computer users play an important role in helping to make the Internet a safer place for everyone. Therefore, the message "security begins at home" should be spread to all computer users.

References

Agostinelli, G. and Grube, J. "Alcohol Counter-advertising and the Media," *Alcohol Research and Health*, Vol. 26, No. 1, 2002, pp. 15-21.

Ajzen, I. "From Intentions to Actions: A Theory of Planned Behavior," in *Action-control: From Cognition to Behavior*, J. Kuhl and J. Beckmann, (eds), Heidelberg: Springer, 1985.

Ajzen, I. *Attitudes, Personality and Behavior*, Milton Keynes, Open University Press, UK, 1988.

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

Ajzen, I., and Driver, B. L. "Application of the Theory of Planned Behavior to Leisure Choice," *Journal of Leisure Research*, 24, 1992, pp. 207-224.

Ajzen, I., Madden, T.I. "Prediction of Goal-Directed Behavior – Attitude, Intentions and Perceived Behavioral Control," *Journal of Experimental Social Psychology*, Vol. 22, 1986, pp. 453-474.

Bagozzi, R. P. and Kimmel, T. F. "A Comparison of Leading Theories for the Prediction of Goal-Directed Behaviors," *British Journal of Social Psychology*, Vol. 34, 1995, pp. 437-461.

Bamberg, S., Ajzen, I. and Schmidt, P. "Choice of Travel Mode in the Theory of Planned Behavior: The Roles of Past Behavior, Habit, and Reasoned Action," *Basic and Applied Social Psychology*, 25(3), 2003, pp. 175-187.

Bandura, A. "Self-efficacy: Towards a Unifying Theory of Behavioral Change," *Psychological Review*, Vol. 84, No. 2, 1977, pp. 191-215.

Bhattacherjee, A. "Acceptance of E-Commerce Services: The Case of Electronic Brokerages," *IEEE Transactions on Systems, Man, and Cybernetics*, Part A, Vol. 30, No. 4, 2000, pp. 411-419.

Boldero, J. "The Prediction of Household Recycling of Newspapers – The Role of Attitudes, Intentions and Situational Factors," *Journal of Applied Social Psychology*, Vol. 25, Iss. 5, 1995, pp. 440-462.

Carpenter, J., Dougherty, C. and Hernan, S. "CERT Advisory CA-2001-20 Continuing Threats to Home Users," 2001. Retrieved March 1, 2005, from http://www.cert.org/advisories/CA-2001-20.html

Chan, K. "Mass Communication and Pro-environmental Behavior: Waste Recycling in Hong Kong," *Journal of Environmental Management*, 52, 1998, pp. 317–325.

Chau, P. and Hu, P. "Information Technology Acceptance by Individual Professionals: A Model Comparison Approach," *Decision Sciences*, Vol. 32, No. 4, Fall 2001, pp. 699-718.

Chin, W. W. "The Partial Least Squares Approach for Structural Equation Modelling," in *Modern Methods for Business Research*, George A. Marcoulides (Ed.), Lawrence Erlbaum Associates, 1998.

Chin, W. W. and Gopal, A. "Adoption Intention in GSS: Relative Importance of Beliefs," *Database*, Vol. 26, No.2&3, 1995, pp. 42-64.

Churchill, G. A. Jr. "A Paradigm for Developing Better Measures of Marketing Constructs," *Journal of Marketing Research*, Vol.6 No.1, February 1979, pp.64-73.

Cohen, J. A. "A Coefficient of Agreement for Nominal Scales," *Educational and Psychological Measurement*, 20, 1960, 37-46.

Cronbach, L. J. “Coefficient Alpha and the Internal Structure of Tests,” *Psychometrika*, Vol. 16, 1951, pp. 297–334.

Davis, F. D. “Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology,” *MIS Quarterly*, Vol. 13, No. 3, September, 1989, pp. 319–340.

Department of Homeland Security. “The National Strategy to Secure Cyberspace,” 2003. Retrieved November 1, 2004, from http://www.dhs.gov/interweb/assetlibrary/National_Cyberspace_Strategy.pdf

Dhillon, G. and Backhouse, J. “Current Directions in IS Security Research: Toward Socio-Organizational Perspectives,” *Information Systems Journal*, Vol 11, No 2, 2001, pp. 127-153.

Dominick, J. R. *The Dynamics of Mass Communication*, Fifth Edition, McGraw-Hill, New York, 1996.

Economist.com. “The Weakest Link,” Oct 2002. Retrieved on October 30, 2004, from http://www.economist.com/printedition/displayStory.cfm?Story_ID=1389553

Falk R. F. and Miller, N. B. *A Primer for Soft Modeling*, The University of Akron Press, Akron, Ohio, 1992.

Fornell, C. & Larcker, V. F. “Evaluating Structural Equation Models with Unobservable Variables and Measurement Error,” *Journal of Marketing Research*, Vol. 18, 1981, pp. 39-50.

Galletta D. F. and Polak P. “An Empirical Investigation of Antecedents of Internet Abuse in the Workplace,” *Proceedings of the Second Annual Workshop on HCI Research in MIS*, Seattle, WA, December 2003, pp. 12-13.

Gefen, D., Straub, D. and Boudreau, M. “Structural Equation Modeling and Regression: Guidelines for Research Practice,” *Communications of the AIS*, Vol.4, No.7, October 2000, pp.1-77.

Hagger, M., Chatzisarantis, N. and Biddle, S. “The Influence of Self-Efficacy and Past Behavior on the Physical Activity Intentions of Young People,” *Journal of Sports Sciences*, 2001, 19, pp. 711-723.

Hair J. F., Anderson R. E., Tatham R. L. and Black W. C. *Multivariate Data Analysis*, Fifth Edition, Prentice-Hall Int. Inc., 1998.

Hartwick, J. and Barki, H. “Explaining the Role of User Participation in Information System Use,” *Management Science*, Vol. 40, Iss. 4, 1994, pp. 405-465.

Internet Usage Statistics. “World Internet Users and Population Stats,” Mar 2005. Retrieved March 24, 2005 from http://www.internetworldstats.com/stats.htm

Johnson R. A. and Wichern D. W. *Applied Multivariate Statistical Analysis*, Fourth edition, Englewood Cliffs, New Jersey, USA, Prentice-Hall, 1998.

Kaiser, F. G., Wolfing S. and Fuhrer, U. “Environmental Attitude and Ecological Behavior,” *Journal of Environmental Psychology*, Vol. 19, 1999, Iss. 1, pp. 1- 19.

Kaiser H. F. “An Index of Factorial Simplicity,” *Psychometrika*, 1974, Vol. 39, pp. 31-36.

Madden, T. J., Ellen, P. S. and Ajzen, I. “A Comparison of the Theory of Planned Behavior and the Theory of Reasoned Action,” *Personality and Social Psychology Bulletin*, Vol. 18, 1992, pp. 3-9.

Mathieson, K. “Predicting User Intentions: Comparing the Technology Acceptance Model with the Theory of Planned Behavior,” *Information Systems Research*, Vol. 2, No.3, September 1991, pp. 173-191.

McQuail, D. *Mass Communication Theory*, Second edition, Sage Publications, London, 1987.

Moore, G. C. and Benbasat, I. “Development of an Instrument to Measure the Perceptions of Adopting an Information Technology Innovation,” *Information Systems Research*, Vol. 2, 1991, pp. 192-222.

Nunnally, J. C. *Psychometric Theory*, Second Edition, McGraw Hill, New York, 1978.

OECD. “OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security,” 2002. Retrieved October 25, 2004, from http://www.oecd.org/dataoecd/16/22/15582260.pdf

OECD. “Understanding the Digital Divide,” 2001. Retrieved June 25, 2004, from http://www.oecd.org/dataoecd/38/57/1888451.pdf

Paviou P. and Fygenson, M. “Understanding and Predicting Electronic Commerce Adoption: An Extension of the Theory of Planned Behavior,” 2004. *MIS Quarterly* (forthcoming).

Reger B., Wootan M., Booth-Butterfield, S. “Using Mass Media to Promote Healthy Eating: A Community-Based Demonstration Project,” *Preventive Medicine*, Vol. 29, 1999, pp. 414-421.

Riemenschneider, C. K., Hardgrave, B. C. and Davis, F. D. “Explaining Software Developer Acceptance of Methodologies: A Comparison of Five Theoretical Models,” *IEEE Transactions on Software Engineering*, Vol. 28, No.12, December 2002, pp. 1135-1145.

Rogers, L. “Home Computer Security,” 2002. Retrieved November 1, 2004, from http://www.cert.org/homeusers/HomeComputerSecurity/

Securitystats.com. “Virus Related Statistics,” 2004. Retrieved Mar 1, 2005, from http://www.securitystats.com/virusstats.html

Sheeran P., Trafimow, D. and Armitage, C. “Predicting Behavior from Perceived Behavioral Control: Tests of the Accuracy Assumption of the Theory of Planned Behavior,” *British Journal of Social Psychology*, 42, 2003, pp. 393–410

Stanton, J. M., Caldera, C., Guzman, I. R., Isaac, A., Lin, P., Mathur, M., Seymour, J., Spitzmueller, C., Stam, K. R., Yamodo, I. and Zakaria, N. “Behavioral Information Security: An Overview, Research Agenda, and Preliminary Results,” *The Security Conference*. Las Vegas, Nevada, April 23-24, 2003.

Taylor, S. and Todd, P. A. “Understanding Information Technology Usage: A Test of Competing Models,” *Information Systems Research*, Vol 6, Issue 2, 1995a, pp. 144-176.

Taylor, S. and Todd, P. A. “An Integrated Model of Waste Management Behavior - A Test of Household Recycling and Composting Intentions,” *Environment and Behavior*, Vol. 27, Iss. 5, 1995b, pp. 603-630.

The Oxford World Encyclopedia. *The Oxford World Encyclopedia*, Oxford University Press, 2001.

Triandis, H. C. *Interpersonal Behavior*, Monterey: Brooks/Cole, 1977.