

PRACTICING SAFE COMPUTING: A MULTIMETHOD EMPIRICAL EXAMINATION OF HOME COMPUTER USER SECURITY BEHAVIORAL INTENTIONS

By: Catherine L. Anderson
Decision, Operations, and Information Technologies
Department
Robert H. Smith School of Business
University of Maryland
Van Munching Hall
College Park, MD 20742-1815
U.S.A.
Catherine_Anderson@rhsmith.umd.edu

Ritu Agarwal
Center for Health Information and Decision Systems
University of Maryland
4327 Van Munching Hall
College Park, MD 20742-1815
U.S.A.
ragarwal@rhsmith.umd.edu

Appendix A

Scales, Items, and Definitions

Concern (Adapted from Ellen and Wiener 1991; Ho 1998; Obermiller 1995)

Anchors 1 = Not At All Concerned, 7 = Very Concerned

Some experts have warned that hackers may try to cripple major American businesses or the government by breaking into their computers, or by using home computers to attack other computers using the Internet. How concerned are you that hackers might...?

- Harm American corporations or the government by breaking into their computers
- Break into home computers and use them to attack computers owned by American corporations or the government
- Break into your home computer and use your e-mail account to send spam to others
- Use home computers to spread a virus over the Internet that harms other computers
- Steal or change data stored on your computer
- Gain access to your personal financial information
- Gain access to your personal health/medical information
- Gain access to other personal data (such as family photos, hobby information, shopping preferences and/or school data)

Security Behavior Self-Efficacy (Adapted from Taylor and Todd 1995)

anchors 1 = Not at all Sure, 7 = Very Confident

For the following questions, security measures are individual actions such as running and updating antivirus software, keeping passwords secure, running a firewall when necessary, etc. Indicate the degree to which you agree or disagree with the following statements:

- I feel comfortable taking measures to secure my primary home computer
- I feel comfortable taking security measures to limit the threat to other people and the Internet in general.
- Taking the necessary security measures is entirely under my control
- I have the resources and the knowledge to take the necessary security measures
- Taking the necessary security measures is easy

Perceived Citizen Efficacy (Adapted from Ellen and Wiener 1991; Ho 1998; Obermiller 1995)

anchors 1 = Strongly Disagree, 7 = Strongly Agree

- If I adopt security measures on my home computer, I can make a difference in helping to secure the Internet
- The efforts of one person are useless in helping secure the Internet
- Every person can make a difference when it comes to helping to secure the Internet
- There is not much that any one individual can do to help secure the Internet

Subjective Norm (Adapted from Taylor and Todd 1995)

anchors 1 = Strongly Disagree, 7 = Strongly Agree

- Friends who influence my behavior would think that I should take measures to secure my primary home computer
- Significant others who are important to me would think that I should take measures to secure my primary home computer
- My peers would think that I should take security measures on my primary home computer to help secure the Internet

Descriptive Norm (newly developed)

anchors 1 = Strongly Disagree, 7 = Strongly Agree

- I believe other people implement security measures on their primary home computers
- I believe the majority of other people take security measures on their primary home computers to help protect the Internet
- I am convinced other people take security measures on their primary home computers
- It is likely that the majority of home computer users take security measures to protect themselves from an attack by hackers

Psychological Ownership for the Internet (Adapted from Dyne and Pierce 2004)

anchors 1 = Strongly Disagree, 7 = Strongly Agree

- The Internet is my network and my data
- I feel a high degree of personal ownership for the Internet
- I sense that the Internet is mine

Psychological Ownership for Own Computer (Adapted from Dyne and Pierce 2004)

anchors 1 = Strongly Disagree, 7 = Strongly Agree

- This is my computer and my data
- I feel a high degree of personal ownership for my computer and data
- I sense that this is my computer

Attitude Toward Performing Security-Related Behavior (Adapted from Taylor and Todd 1995)

anchors 1 = Strongly Disagree, 7 = Strongly Agree

- Security measures such as implementing anti-virus software, firewalls, or system updates on your home computer are a good idea
- Taking security measures to protect your home computer is important
- I like the idea of taking security measures to secure my home computer

Intentions to Perform Security-Related Behavior (Internet) – (Adapted from Taylor and Todd 1995)

anchors 1 = Strongly Disagree, 7 = Strongly Agree

Thinking of your future actions, indicate the degree to which you agree or disagree with the following statements regarding your likelihood of implementing security measures to protect YOUR PRIMARY HOME COMPUTER from an attack by hackers

- I am likely to take security measures on my home computer to protect the Internet
- It is possible that I will take security measures on my home computer to protect the Internet
- I am certain that I will take security measures on my home computer to protect the Internet

*Intentions to Perform Security-Related Behavior (Own Computer) (Adapted from Taylor and Todd 1995)**anchors 1 = Strongly Disagree, 7 = Strongly Agree*

Thinking of your future actions, indicate the degree to which you agree or disagree with the following statements regarding your likelihood of implementing security measures on your primary home computer to help protect THE INTERNET from an attack by hackers

- I am likely to take security measures to protect my primary home computer
- It is possible that I will take security measures to protect my primary home computer
- I am certain that I will take security measures to protect my primary home computer

Controls

- (1) Gender: 1 = male; 2 = female.
- (2) Age: 1 = Under 18; 2 = 18–24; 3 = 25–34; 4 = 35–44; 5 = 45–54; 6 = 55–64; 7 = over 65 years.
- (3) Education: 1 = Some school, no degree; 2 = High School Graduate; 3 = Some college, no degree; 4 = Associate's Degree; 5 = Bachelor's Degree; 6 = Master's Degree; 7 = Doctoral Degree.
- (4) Internet experience: 1 = Less than 1 year; 2 = 1 year–5 years; 3 = 6 years–10 years; 4 = 11 years–15 years; 5 = More than 15 years.
- (5) Security violation victim: How frequently have you personally been affected by a security violation? 1 = Very infrequently; 7 = Very frequently.
- (7) Media exposure: How much have you heard or read during the last year about security violations (e.g., threats such as virus attacks and/or unauthorized access to data by hackers)? 1 = Not at all; 7 = Very much.

References

- Dyne, L., and Pierce, J. 2004. "Psychological Ownership and Feelings of Possession: Three Field Studies Predicting Employee Attitudes and Organizational Citizenship Behavior," *Journal of Organizational Behavior* (25), pp. 439-459.
- Ellen, P. S., and Wiener, J. L. 1991. "The Role of Perceived Consumer Effectiveness in Motivating," *Journal of Public Policy & Marketing* (10:2), pp. 102-117.
- Ho, R. 1998. "The Intention to Give Up Smoking: Disease Versus Social Dimensions," *Journal of Social Psychology* (138:3), pp. 368-380.
- Obermiller, C. 1995. "The Baby Is Sick/The Baby Is Well: A Test of the Environmental Communication Appeals," *Journal of Advertising* (24:2), pp. 55-71.
- Taylor, S., and Todd, P. 1995. "Understanding Information Technology Usage: A Test of Competing Models," *Information Systems Research* (6:2), pp. 144-176.

Appendix B

Common Method Bias Analysis

In an effort to limit the susceptibility of the study to common methods bias, we provided contextual information and definitions to potentially ambiguous or unfamiliar terms within the survey. In addition, as suggested by Podsakoff et al. (2003), at the beginning of the online survey, the respondents read a statement informing them that there are no right or wrong answers to the questions and that they should respond as honestly as possible. Their anonymity was assured as no identifying information was gathered as part of the survey. We also conducted statistical tests to assess potential common methods bias in our results. First, as discussed by Podsakoff et al., we performed an exploratory factor analysis which yielded 10 separate factors (consistent with the number of constructs in the model). No single factor explains the majority of covariance among the measures, indicating that common method biases do not present a significant problem with the data. Second, following Podsakoff et al. and Williams et al. (2003), we included a common method factor in our PLS model in a manner consistent with Liang et al. (2007). As shown below, the results indicate that the average variance explained by the substantive indicators is .768 while the average method-based variance is .011. Given the small magnitude of the method variance, we conclude that method bias is not a threat for this study.

Construct	Indicator	Substantive Factor Loading (R1)	R1	Method Factor Loading (R2)	R2
Psychological Ownership (Computer)	POC1	.965	.931**	-.024	.001
	POC2	.946	.895**	.015	.000
	POC3	.937	.878**	.009	.000
Psychological Ownership (Internet)	POI1	.919	.845**	.024	.001
	POI2	.967	.935**	.006	.000
	POI3	.953	.908**	-.029	.001
Self-Efficacy	SE1	.807	.651**	.108	.012**
	SE2	.792	.627**	.138	.019**
	SE3	.868	.753**	-.056	.003
	SE4	.822	.676**	-.092	.008**
	SE5	.895	.801**	-.105	.011**
Subjective Norm	SN1	.956	.914**	-.056	.003**
	SN2	.914	.835**	.035	.001**
	SN3	.934	.872**	.021	.000
Descriptive Norm	DN1	.843	.711**	-.001	.000
	DN2	.861	.741**	.191	.036
	DN3	.919	.845**	-.049	.002
	DN4	.868	.753**	.013	.000
Concern	CONC1	.635	.403**	-.027	.001**
	CONC2	.731	.534**	.037	.001
	CONC3	.861	.741**	-.075	.006**
	CONC4	.707	.500**	.134	.018**
	CONC5	.874	.764**	-.024	.001
	CONC6	.833	.694**	-.015	.000
	CONC7	.877	.769**	0.052	.003
	CONC8	.901	.812**	0.096	.009**
Perceived Citizen Effectiveness	PCE1	.630	.397**	.300	.090**
	PCE2	.921	.848**	-.254	.065**
	PCE3	.692	.479**	.206	.042**
	PCE4	.955	.912**	-.263	.069**
Attitude	ATT1	.966	.933**	-.066	.004**
	ATT2	.961	.924**	-.027	.001
	ATT3	.784	.615**	.099	.010**
Intentions (Computer)	INTC1	.917	.841**	.021	.000
	INTC2	.887	.787**	-.059	.003
	INTC3	.893	.797**	.033	.001
Intentions (Internet)	INTI1	.943	.889**	.006	.000
	INTI2	.945	.893**	-.035	.001
	INTI3	.925	.856**	.028	.001
Average		.872	.768	.008	.011

References

- Liang, H., Saraf, N., Hu, Q., and Xue, Y., 2007. "Assimilation of Enterprise Systems: The Effect of Institutional Pressures and the Mediating Role of Top Management," *MIS Quarterly* (31:1), pp. 59-87.
- Podsakoff, P. M., MacKenzie, S. B., Leong-Yeon, L., and Podsakoff, N. P. 2003. "Common Method Biases in Behavioral Research: A Critical Review of the Literature and Recommended Remedies," *Journal of Applied Psychology* (88:5), pp. 879-903.
- Williams, L. J., Edwards, J. R., and Vandenberg, R. J. 2003. "Recent Advances in Causal Modeling Methods for Organizational and Management Research," *Journal of Management* (29:6). 2003, pp. 903-936.

Appendix C

Psychometric Properties of Measurement Scales for Study 1

The composite reliability scores for the reflective constructs shown in Table C1 indicate the scales used meet the generally accepted .70 or greater guideline. A comparison of interconstruct correlations and average variance extracted (shaded diagonal), also provided in Table C1, indicate that the reflective constructs demonstrate convergent and discriminant validity as all constructs share more variance with their own indicators than with those of other constructs. A confirmatory factor analysis (CFA) performed in PLS suggests convergent and discriminant validity of the scales (Table C2). Although there are some correlations that exceed 0.5, as noted by Gefen and Straub (2005), the fact that items load much higher on their constructs satisfactorily demonstrates convergent and discriminant validity. Loadings produced in PLS are commonly higher than in a principal component analysis (Gefen and Straub 2005); therefore, we also conducted a principal component analysis (PCA) on the data in SPSS. While the results of this analysis show marginally lower loadings of all items on their appropriate factors, all except two exceed .7 and there are no cross loadings above .4 (Table C3). The two lower loadings shown on the PCA analysis may reflect an artifact of the mixed positive and negative item wording within the perceived citizen effectiveness scale, which contains two reverse coded items (Deemer and Minke 1999). These differences in loadings between factor analysis methods are consistent with comparisons conducted by Gefen and Straub. Collectively, these tests confirm satisfactory validity of the reflective scales.

As recommended by Petter et al. (2007), when assessing the validity of formative constructs using a component based SEM such as PLS, the model weights should be examined. Table C4 presents the item weights and t-statistics for the items comprising the concern formative construct. Five of the eight items are significant. To maintain content validity, the three nonsignificant items are retained for subsequent analysis (Petter et al. 2007). To assess discriminant validity of the formative scale and further examine its convergent validity we adopted an approach similar to that used by Loch et al. (2003), which is based on a variation of Campbell and Fiske's (1959) multitrait-multimethod analysis. We multiplied each of the concern item values by their individual PLS weights and summed them up to obtain a composite score for the concern construct, which is consistent with Bagozzi and Fornell (1982). Using the weighted item scores and the composite scores, we ran inter-item correlations and item-to-construct correlations to create a matrix of these values shown in Table C5.

To assess discriminant validity, we included the items and construct scores for two additional constructs, perceived citizen effectiveness and self-efficacy, in the correlation matrix. Inter-item and item-to-construct correlations should demonstrate a stronger correlation to each other than to measures of other constructs. The inter-item correlations and the item-to-construct correlations for the concern construct are all significant at the .01 level suggesting convergent validity of the instrument. With the exception of the Conc8 item correlation with the composite concern variable, all of the correlations within the concern construct are higher than the correlations between the concern items and any of the self-efficacy and perceived citizen effectiveness items or related construct scores, which is persuasive evidence for overall discriminant validity of the concern formative measure. The Conc8 exception suggests that this item is not as strong as the other measures of concern as it appears to correlate with two of the perceived citizen effectiveness items. It does, however, have a stronger correlation with the composite concern variable than it does to the perceived citizen effectiveness construct score.

References

- Bagozzi, R. P., and Fornell, C. 1982. "Theoretical Concepts, Measurement, and Meaning," in *A Second Generation of Multivariate Analysis*, C. Fornell (ed.), New York: Praeger, (2), pp. 5-23.
- Campbell, D. T., and Fiske, D. W. 1959. "Convergent and Discriminant Validation by the Multitrait-Multimethod Matrix," *Psychological Bulletin* (56), pp. 81-105.
- Deemer, S. A., and Minke, K. M. 1999. "An Investigation of the Factor Structure of the Teacher Efficacy Scale," *Journal of Educational Research* (93:1), pp. 3-10.
- Gefen, D., and Straub, D. 2005. "A Practical Guide to Factorial Validity Using PLS-Graph: Tutorial and Annotated Example," *Communications of the Association for Information Systems* (16), pp. 91-109.
- Loch, K., Straub, D., and Kamel, S. 2003. "Diffusing the Internet in the Arab World: The Role of Social Norms and Technological Culturation," *IEEE Transactions on Engineering Management* (50:1), pp. 45-63.
- Petter, S., Straub, D., and Rai, A. 2007. "Specifying Formative Constructs in Information Systems Research," *MIS Quarterly* (31:4), pp. 623-656.

Table C1. Interconstruct Correlations

Construct	Reliability (# of items)	Concern	PCE	Attitude	SelfEff	SubjNorm	DescNorm	PsychOwn (Internet)	Intentions (Internet)	Intentions (Computer)	PsychOwn (Computer)
PCE	.81(4)	.27	.79								
Attitude	.88(3)	.46	.36	.91							
SelfEff	.91(5)	.13	.32	.41	.86						
SubjNorm	.92(3)	.17	.11	.13	.09	.93					
DescNorm	.90(4)	.19	.14	.18	.19	.21	.87				
PsychOwn (Internet)	.94(3)	.09	.15	-.02	.11	.11	.23	.95			
Intentions (Internet)	.93(3)	.27	.51	.43	.38	.13	.23	.21	.94		
Intentions (Computer)	.86(3)	.31	.31	.64	.44	.21	.18	.01	.52	.90	
PsychOwn (Computer)	.94(3)	.19	.18	.21	.12	.08	.03	.17	.11	.19	.95

Table C2. Confirmatory Factor Analysis

	PCE	ATT	SE	SN	DN	POI	INTI	INTC	POC
POC1									.957
POC2									.957
POC3									.933
POI1						.937			
POI2						.966			
POI3						.935			
SE1		.469	.905					.469	
SE2			.898				.423	.410	
SE3			.808						
SE4			.882						
SE5			.798						
SN1				.928					
SN2				.935					
SN3				.941					
DN1					.839				
DN2					.902				
DN3					.875				
DN4					.868				
PCE1	.859						.503		
PCE2	.708								
PCE3	.852						.491		
PCE4	.741								
ATT1		.916						.571	
ATT2		.940						.607	
ATT3		.859	.411				.414	.559	
INTC1		.611	.416				.489	.933	
INTC2		.488					.442	.841	
INTC3		.617	.457				.476	.918	
INTI1	.492	.407					.947	.488	
INTI2	.438						.921	.503	
INTI3	.509	.431	.402				.945	.479	

Notes: CONC = Concern; PCE = Perceived Citizen Effectiveness; ATT = Attitude; SE = Self Efficacy; SN = Subjective Norm; DN = Descriptive Norm; POI = Psychological Ownership (Internet); INTI = Intentions (Internet); INTC = Intentions (Computer); POC = Psychological Ownership (Computer). Bold numbers indicate item loadings on assigned constructs.

Numbers presented in this table represent bivariate Pearson correlations between item scores and latent variable scores produced by PLS.

	PCE	ATT	SE	SN	DN	POI	INTI	INTC	POC
POC1									.946
POC2									.936
POC3									.928
POI1						.899			
POI2						.954			
POI3						.930			
SE1			.795						
SE2			.799						
SE3			.835						
SE4			.898						
SE5			.836						
SN1				.931					
SN2				.908					
SN3				.930					
DN1					.839				
DN2					.845				
DN3					.885				
DN4					.854				
PCE1	.586								
PCE2	.860								
PCE3	.602								
PCE4	.884								
ATT1		.862							
ATT2		.870							
ATT3		.732							
INTC1								.765	
INTC2								.810	
INTC3								.720	
INTI1							.852		
INTI2							.852		
INTI3							.846		

Extraction Method: Principal Component Analysis
 Rotation Method: Varimax with Kaiser Normalization

Item	Weight	t-stat
Conc1	.483***	4.539
Conc2	-.256*	-1.968
Conc3	-.262	-1.793
Conc4	.901***	8.391
Conc5	-.049	-.330
Conc6	.370*	2.215
Conc7	-.029	-.193
Conc8	-.251*	-2.190

Table C5. Inter-Item and Item-to-Construct Correlation Matrix

	Conc 1	Conc2	Conc3	Conc4	Conc5	Conc6	Conc7	Conc8	Conc	SE1	SE2	SE3	SE4	SE5	Self Eff
Conc1	—														
Conc2	-.727**	—													
Conc3	-.490**	.598**	—												
Conc4	.595**	-.629**	-.666**	—											
Conc5	-.468**	.522**	.667**	-.637**	—										
Conc6	.465**	-.451**	-.568**	.559**	-.721**	—									
Conc7	-.471**	.508**	.583**	-.515**	.699**	-.769**	—								
Conc8	-.443**	.472**	.625**	-.532**	.735**	-.690**	.809**	—							
Conc	.667**	-.407**	-.293**	.810**	-.401**	.545**	-.324**	-.221**	—						
SE1	.155**	-.112**	-.081	.146**	-.119**	.133**	-.098*	-.043	.186**	—					
SE2	.163**	-.159**	-.092*	.150**	-.138**	.138**	-.123**	-.072	.165**	.807**	—				
SE3	.059	-.055	-.044	.092*	-.071	.064	-.064	-.047	.089*	.595**	.640**	—			
SE4	.042	-.055	-.004	.060	-.016	.064	-.061	-.011	.081*	.710**	.684**	.724**	—		
SE5	-.016	-.017	.035	-.021	-.018	.015	-.034	-.020	-.023	.601**	.602**	.633**	.760**	—	
SE	.081	-.088*	-.047	.090*	-.086*	.086*	-.081	-.044	.096*	.837**	.838**	.828**	.902**	.843**	—
PCE1	.317**	-.309**	-.236**	.300**	-.251**	.244**	-.274**	-.2488**	.256**	.361**	.409**	.281**	.310**	.235**	.317**
PCE2	.091*	-.037	.001	.065	-.018	.087*	-.082*	-.046	.115**	.141**	.165**	.076	.061	.038	-.034
PCE3	.279**	-.309**	-.219**	.266**	-.219	.207**	-.261**	-.234**	.202**	.296**	.354**	.245**	.248**	.209**	.254**
PCE4	.094*	-.067	.008	.078	.006	.067	-.056	-.009	.129**	.167**	.188**	.071	.065	.003	-.031
PCE	.232**	-.207**	-.127**	.207**	-.134**	.176**	-.193**	-.152**	.211**	.196**	.254**	.076	.065	0	0

	PCE1	PCE2	PCE3	PCE4	PCE
Conc1					
Conc2					
Conc3					
Conc4					
Conc5					
Conc6					
Conc7					
Conc8					
ConcW					
SE1					
SE2					
SE3					
SE4					
SE5					
SE					
PCE1	—				
PCE2	.387**	—			
PCE3	.713**	.407**	—		
PCE4	.441**	.718**	.436**	—	
PCE	.731**	.819**	.746**	.849**	—

ConcW is the Concern construct weighted composite score

**Correlation is significant at the 0.01 level (2-tailed)

*Correlation is significant at the 0.05 level (2-tailed)

Appendix D

Operationalization of Survey and Experiment

Definitions Provided to Survey Respondents and Experiment Subjects

- *Security violations* include threats such as virus attacks and/or unauthorized access to data by hackers.
- *Cybersecurity* is a general term indicating the safety and health of the Internet including the computers, communication lines, programs and data that enable and support the Internet.
- *Security measures* are individual actions such as running and updating antivirus software, keeping passwords secure, running a firewall when necessary, and exercising care when opening e-mail attachments.

Experimental Website Conditions

Prevention/Independent Condition (1)

How You Can Become a Conscientious Cybercitizen

The Internet has made it easier for hackers to spread computer viruses or to commit other illegal acts involving computers in homes, businesses or government agencies. With the U.S. Census reporting in 2001 that over half of U.S. households contain a computer with Internet access, the American population has unprecedented access to the resources of this global network from their own homes. Your behavior and habits can impact the security and privacy of your own personal data and potentially compromise the safety of the Internet technology.

Many companies provide hardware and software to minimize the risk of security breaches. However, technology alone is not the solution to the cyber security problem. You must be aware of the security issue and practice appropriate security behaviors on their home computers.

What Can You Do?	Personal Consequences
<ul style="list-style-type: none"> • Use "anti-virus software" and keep it up to date. • Don't open emails or attachments from unknown sources • Protect your computer from Internet intruders – use "firewalls." • Regularly download security updates and "patches" for your operating systems and other software. • Use hard-to-guess passwords. Mix upper case, lower case, numbers, or other characters not easy to find in a dictionary, and make sure they are at least eight characters long. • Don't share access to your computers with strangers. • Disconnect from the Internet when not in use. 	<ul style="list-style-type: none"> • Lost personal information on home PC • Unauthorized access to your personal information (identity theft) • Use of your computer to send spam or spread viruses to friends and family • Use of your computer as a bot to send overload servers with requests (Denial of Service attack) • Decreased confidence in using the internet to conduct personal research and business transactions (i.e. providing information to trusted sources) • Unavailability of Internet resources for conducting personal research and business transactions


*Avoid the personal consequences of security violations -
Protect yourself by following these suggested secure online behaviors!*

You must do your part in the effort to secure this vital, global network for your future.

Prevention /Interdependent Condition (2)

Creating Conscientious Cybercitizens - Mozilla Firefox

How All Inter-Connected Users of the Internet Can Become Conscientious Cybercitizens



The Internet has made it easier for hackers to spread computer viruses or to commit other illegal acts involving computers in homes, businesses or government agencies. With the U.S. Census reporting in 2001 that over half of U.S.households contain a computer with Internet access, the American population has unprecedented access to the shared resources of this global network from their own homes. The behavior and habits of each inter-connected user of the Internet can impact the security and privacy of the the data of all Internet users and potentially compromise the safety of the Internet technology.

Many companies provide hardware and software to minimize the risk of security breaches. However, technology alone is not the solution to the cyber security problem. All members of the Internet community must be aware of the security issue and practice appropriate security behavior on their home computers.

What Can All Interconnected-Users Do?	Internet Community Consequences
<ul style="list-style-type: none"> • Use "anti-virus software" and keep it up to date. • Don't open emails or attachments from unknown sources • Protect each computer from Internet intruders – use "firewalls." • Regularly download security updates and "patches" for operating systems and other software. • Use hard-to-guess passwords. Mix upper case, lower case, numbers, or other characters not easy to find in a dictionary, and make sure they are at least eight characters long. • Don't share access to computers with strangers. • Disconnect from the Internet when not in use. 	<ul style="list-style-type: none"> • Lost information on Internet connected PCs • Unauthorized access to information (identity theft) • Use of connected computers to send spam or spread viruses to other Internet users • Use of connected computers as bots to overload servers with requests (Denial of Service attack) • Decreased confidence in using the internet to conduct research and business transactions (i.e. providing information to trusted sources) • Unavailability of Internet resources for conducting research and business transactions


Avoid the consequences to the community of Internet users from security violations – Protect your community by following these suggested secure online behaviors!

We all must do our part in the effort to secure this vital, global network for the future.

Promotion/Independent Condition (3)

Becoming a Conscientious Cybercitizen - Mozilla Firefox

How You Can Become a Conscientious Cybercitizen



The Internet has made it easier for hackers to spread computer viruses or to commit other illegal acts involving computers in homes, businesses or government agencies. With the U.S. Census reporting in 2001 that over half of U.S.households contain a computer with Internet access, the American population has unprecedented access to the shared resources of this global network from their own homes. Your behavior and habits can impact the security and privacy of your own personal data and potentially compromise the safety of the Internet technology.

Many companies provide hardware and software to minimize the risk of security breaches. However, technology alone is not the solution to the cyber security problem. You must be aware of the security issue and practice appropriate security behavior on your home computer.

What Can You Do?	Personal Benefits
<ul style="list-style-type: none"> • Use "anti-virus software" and keep it up to date. • Don't open emails or attachments from unknown sources • Protect your computer from Internet intruders – use "firewalls." • Regularly download security updates and "patches" for your operating systems and other software • Use hard-to-guess passwords. Mix upper case, lower case, numbers, or other characters not easy to find in a dictionary, and make sure they are at least eight characters long. • Don't share access to your computer with strangers. • Disconnect from the Internet when not in use. 	<ul style="list-style-type: none"> • Increased confidence in storing your personal information on home PCs • Increased privacy - Only authorized access to your personal information • Confidence that your computer will not be unwittingly used to participate in the spread of spam or viruses to Internet users • Confidence that your computer will not be unwittingly used as a bot to overload servers with requests (Denial of Service attacks) • Increased trust in using the internet to conduct personal research and business transactions • Access to Internet resources for conducting personal research and business transactions

Enjoy the confidence of knowing you are doing your part to secure cyberspace - Reap the benefits by following these suggested secure online behaviors!

Your action is needed to gain the full benefits of this vital, global network for the future.

Promotion/Interdependent Condition (4)

How All Inter-Connected Users of the Internet Can Become Conscientious Cybercitizens

The Internet has made it easier for hackers to spread computer viruses or to commit other illegal acts involving computers in homes, businesses or government agencies. With the U.S. Census reporting in 2001 that over half of U.S. households contain a computer with Internet access, the American population has unprecedented access to the shared resources of this global network from their own homes. The behavior and habits of each inter-connected user of the Internet can impact the security and privacy of the data of all Internet users and potentially compromise the safety of the Internet technology.

Many companies provide hardware and software to minimize the risk of security breaches. However, technology alone is not the solution to the cyber security problem. The members of the Internet community must be aware of the security issue and practice appropriate security behavior on their home computers.

What Can All Inter-Connected Users Do?	Internet Community Benefits
<ul style="list-style-type: none"> • Use "anti-virus software" and keep it up to date. • Don't open emails or attachments from unknown sources. • Protect each computer from Internet intruders – use "firewalls." • Regularly download security updates and "patches" for operating systems and other software. • Use hard-to-guess passwords. Mix upper case, lower case, numbers, or other characters not easy to find in a dictionary, and make sure they are at least eight characters long. • Don't share access to computers with strangers. • Disconnect from the Internet when not in use. 	<ul style="list-style-type: none"> • Increased confidence in storing information on Internet-connected PCs • Increased privacy - Only authorized access to information on the Internet • Confidence that computers will not be unwittingly used to participate in the spread of spam or viruses to Internet users • Confidence that connected computers will not be unwittingly used as bots to overload servers with requests (Denial of Service attacks) • Increased trust in using the internet to conduct research and business transactions • Access to of Internet resources for conducting research and business transactions

*Enjoy the confidence of knowing we are all doing our part to secure cyberspace -
Reap the benefits by following these suggested secure online behaviors!*

We all must do our part to gain the full benefits of this vital, global network for the future.

Appendix E

Manipulation Check Items

Manipulation Checks: Self-View

While you were reviewing the website about the security issue and becoming a conscientious cybercitizen, please describe the extent to which:

You thought about yourself

Not at all 1 — 2 — 3 — 4 — 5 — 6 — 7 A lot

Your thoughts about the security issue were focused on just yourself

Not at all 1 — 2 — 3 — 4 — 5 — 6 — 7 A lot

Your thoughts were focused on just you

Not at all 1 — 2 — 3 — 4 — 5 — 6 — 7 A lot

You thought about other users of the Internet

Not at all 1 — 2 — 3 — 4 — 5 — 6 — 7 A lot

Your thoughts about the security issue were focused on other users of the Internet

Not at all 1 — 2 — 3 — 4 — 5 — 6 — 7 A lot

Your thoughts were focused on other users of the Internet

Not at all 1 — 2 — 3 — 4 — 5 — 6 — 7 A lot

Manipulation Checks: Goal Frame

While you were reviewing the website about the security issue and becoming a conscientious cybercitizen, please describe the extent to which you agree or disagree with the following statements:

The website made me think about the benefits of following recommended security behaviors

Strongly Disagree 1 — 2 — 3 — 4 — 5 — 6 — 7 Strongly Agree

The website made me think about the benefits of a secure Internet environment

Strongly Disagree 1 — 2 — 3 — 4 — 5 — 6 — 7 Strongly Agree

The website made me think about the consequences of security violations

Strongly Disagree 1 — 2 — 3 — 4 — 5 — 6 — 7 Strongly Agree

The website made me think about the consequences of not performing the recommended security behaviors

Strongly Disagree 1 — 2 — 3 — 4 — 5 — 6 — 7 Strongly Agree

Appendix F

Psychometric Properties of Measurement Scales for Study 2

Items	Descriptive Norm	Subjective Norm	Attitude (Computer)	Attitude (Internet)
DN1	.812	.308	.150	-.011
DN2	.918	.050	-.041	-.063
SN1	.266	.854	.030	-.087
SN2	.328	.808	.137	-.008
SN3	-.139	.825	-.037	.262
ATTC1	.053	.038	.929	.122
ATTC2	.077	.004	.965	.038
ATTC3	-.014	.077	.922	.090
ATTINT1	.023	.084	.053	.906
ATTINT2	-.038	-.053	.159	.898
ATTINT3	-.063	.080	.031	.710

Extraction Method: Principal Component Analysis

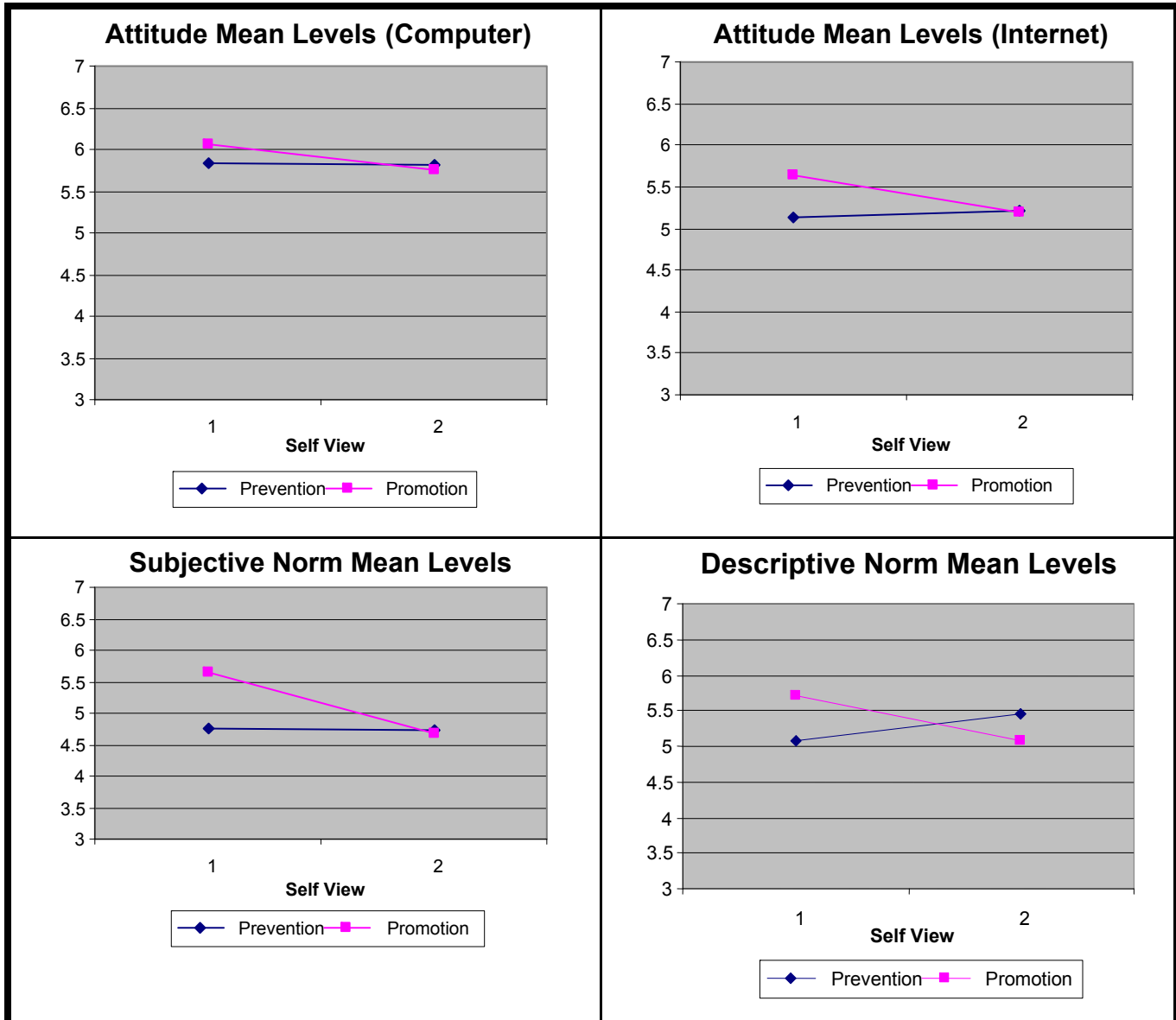
Rotation Method: Varimax with Kaiser Normalization

Bold numbers indicate item loadings on assigned constructs

Construct	Reliability (number of items)
Subjective Norm	.80(3)
Descriptive norm	.76(2)
Attitude Toward Performing Security-Related Behavior: Own Computer	.94(3)
Attitude Toward Performing Security-Related Behavior: Internet	.80(3)

Appendix G

Interaction Graphs and Table of Means for Study 2 Outcome Variables



The independent self view condition is coded 1 (interdependent is 2).

Figure G1. Interaction Graphs Depicting Outcome Variable Means by Self View and Goal Frame

Table G1. Study 2 Cell Means

Self View	Goal Frame		Attitude (Computer)	Attitude (Internet)	Subjective Norm	Descriptive Norm
Independent	Promotion	Mean	6.067	5.627	5.640	5.720
		N	25	25	25	25
		Std. Dev.	1.732	1.230	1.182	1.119
	Prevention	Mean	5.747	5.200	4.747	5.080
		N	25	25	25	25
		Std. Dev.	1.310	1.110	1.362	1.305
Interdependent	Promotion	Mean	5.840	5.133	4.667	5.080
		N	25	25	25	25
		Std. Dev.	1.248	.892	1.302	1.367
	Prevention	Mean	5.808	5.218	4.718	5.462
		N	26	26	26	26
		Std. Dev.	1.418	1.445	1.246	1.148

Appendix H

Rationale for Research Approach and Future Research Opportunities

In this appendix, we provide a brief rationale for the selected research approach, as well as suggest directions in which the studies reported here could be extended.

Our overarching goal in this research was to broadly understand the phenomenon of individual security motivations including whether and how they may be influenced, while simultaneously balancing the demands of rigor and relevance. Numerous scholars have commented on the issue of relevance in information systems research (Benbasat and Zmud 1999; Davenport and Markus 1999; Klein et al. 2006; Roseman and Vessey 2008; Senn 1998). Some have adopted the stance that it is difficult to simultaneously achieve rigor and relevance with a study (see, for example, Davenport and Markus 1999) while others have proposed solutions for improving the degree of relevance in IS research (Benbasat and Zmud 1999; Roseman and Vessey 2008). Our solution here was to combine scientific rigor with practical relevance using a two-phased, multimethod research program consistent with Senn's (1998) recommendation to focus "on a continuing series of efforts using a mix of methods" to ensure relevance in IS research.

While there are theoretical contributions made as a result of both studies 1 and 2, the individual security motivation model which we build and test in study 1 represents the major theoretical contribution of this paper. However, in isolation, the findings from study 1 fall short of providing the concrete recommendations and guidance to make the findings relevant for practice (Klein et al. 2006). Thus, we designed the experiment conducted as study 2 based on the findings of the survey conducted in study 1. The experimental setting we chose for study 2 provides the control necessary to establish causality and more definitive guidelines regarding how to influence the factors identified as important in forming security behavior.

Future Directions

Behavioral aspects of security are understudied in the information systems literature and, in addition to the work suggested by the theoretical implications of the two studies, several opportunities for fruitful future research remain. One interesting area for research would be to examine why some people feel more of a sense of ownership toward the Internet than others. Perhaps national culture has some explanatory power here, or individual demographic characteristics. It may also be the case that an individual's dependence on the Internet for social support is influential in determining how much he/she feels a sense of ownership.

A second recommended area of future research would be to further explore the differences in behavior between employees and home users. Do people behave differently at work than at home with regard to security measures? It would be interesting to conduct research to assess whether an employee's level within the organization has any impact on security behavior. One might suspect that psychological ownership toward company data, computers and technical infrastructure is greater for employees higher up in the organization's hierarchy.

Future research could examine the various forms of media and their effectiveness at increasing the desired security behavior. Still other studies could focus on identifying potential moderators to our model, including determining the role of habit (Kim et al. 2005) and events or responses that result in a false sense of security (Kahn and Luce 2006). An understanding of the types of behavioral responses people have may also inform organizations regarding the type of awareness and training required to change these behaviors.

References

- Benbasat, I., and Zmud, R. W. 1999. "Empirical Research in Information Systems: The Practice of Relevance," *MIS Quarterly* (23:1), pp. 3-16.
- Davenport, T.H., and Markus, M. L. 1999. "Rigor vs. Relevance Revisited: Response to Benbasat and Zmud," *MIS Quarterly* (23:1), pp. 19-23.
- Kahn, B. E., and Luce, M. F. 2006. "Repeated-Adherence Protection Model: "I'm Ok, and It's a Hassle," *American Marketing Association* (25:1), pp. 79-89.
- Kim, S. S., Malhotra, N. K., and Narasimhan, S. 2005. "Two Competing Perspectives on Automatic Use: A Theoretical and Empirical Comparison," *Information Systems Research* (16:4), pp. 418-432.
- Klein, G., Jiang, J.J., and Saunders, C. 2006. "Leading the Horse to Water" *Communications of the AIS* (18), pp. 259-274.
- Rosemann, M., and Vessey, I. 2008. "Toward Improving the Relevance of Information Systems Research to Practice: The Role of Applicability Checks," *MIS Quarterly* (32:1), pp. 1-22.
- Senn, J. 1998. "The Challenge of Relating IS Research to Practice," *Information Resources Management Journal* (11:1), pp. 23-28.