2013

College Student Home Computer Security Adoption

Chet L. Claar

Robert C. Shields

David Rawlinson

Robert Lupton

Issues in Information Systems
Volume 14, Issue 2, pp.139-148, 2013

COLLEGE STUDENT HOME COMPUTER SECURITY ADOPTION

Chet L. Claar, Central Washington University, claar@cwu.edu
Robert C. Shields, Central Washington University, lymrcs@ieee.org
David Rawlinson, Central Washington University, rawlinsd@cwu.edu
Robert Lupton, Central Washington University, luptonr@cwu.edu

ABSTRACT

The home Internet user faces a hostile environment abundant in potential attacks on their computers. These attacks have been increasing at an alarming rate and cause damage to individuals and organizations regularly, and have the potential to cripple the critical infrastructures of entire countries. Recent research has determined that some individuals are not utilizing additional software protections available to mitigate these potential security risks. This paper seeks to clarify the reasons by proposing a conceptual framework that utilizes the Health Belief Model as a possible way to explain why some people do not perceive a threat sufficient to prompt the adoption of computer security software.

Keywords: computer security, technology adoption, home computer security, health belief model and protective technology

INTRODUCTION

This paper uses the Security Adoption Behavior Model (SABM) presented in [4] to assess home computer security adoption by students at a medium sized public university in Washington. There are striking similarities in the beliefs and perceptions in protecting one's health and in protecting one's computer from infection and attack. The SABM uses constructs from the long standing medical Health Belief Model presented in [10]. The objective of the current work is to better understand why individuals do (or do not) adopt better security behaviors and ultimately to understand how to increase their motivation to do so.

Research [1, 6] has consistently found that some people do not use available software to reduce their security risk. The phenomenal growth of the Internet has brought new and exciting opportunities to the home computer user. Online shopping and banking, communication with friends and relatives, access to sources of information for research and homework, entertainment sources, up-to-the-minute weather and news, and countless other possible online activities have made the internet indispensible for most online-enabled households. However, while providing these new opportunities for home Internet users, it has also provided an opportunity-rich environment for criminals and others with malicious intent. They seek to exploit computer users who do not adequately protect themselves from the ever-increasing number of cyber threats. Using computer security solutions available in the form of anti-virus, anti-spyware, and firewall software in addition to ensuring that operating systems are properly updated provides effective protection from these online threats.

The U.S. Census Bureau statistics for 2010 population survey show over 119.5 million households in the United States with Internet access [12]; all of these are potential targets for Internet-borne attacks. Consumer Reports surveyed home users in 2012 and extrapolating from their data estimate 58.2 million online users suffered a noticeable malware infection [6].

America Online and the National Cyber Security Alliance conducted a survey of Internet users in the United States in order to assess their level of security awareness and good practice [1]. The study revealed that approximately 75% of all respondents feel that their computer is very safe from online attacks and viruses. Thus, 84% of respondents keep sensitive information on their computer and 72% use their computers for sensitive transactions. An examination of the respondents' systems revealed that 15% had no anti-virus software installed and that 67% were not updated within the previous week, 19% of these computers had an active viral infection, and that 63% had experienced a previous viral infection. The study discovered that 67% of computers had no firewall software installed, and 72% with firewalls installed were not properly configured.-Inadequately protected computers represented by these recent studies equate to millions of vulnerable computers in the United States that are potential victims. With the possibility of infected machines being used to disrupt or destroy critical infrastructures and disrupt vital services, the necessity of determining the factors involved in the adoption of computer security solutions continues to be important.

LITERATURE REVIEW

The behavioral antecedents of adoption and use of computer security solutions of home computer users is the focus of this research. The concept of perceived vulnerability in online activities seems an appropriate aspect to examine when trying to understand adoption and usage behavior for computer security solutions. Additionally, the severity of a security incident to the user would also be an important user perception to examine in an effort to better understand adoption behavior. Focusing this research on the individual home computer user will contribute to a better understanding of computer security adoption behavior.

The current predominant models in information systems used to examine user adoption and usage behavior are the Theory of Reasoned Action [8], the Theory of Planned Behavior [2], the Technology Acceptance Model [7], the Unified Theory of Acceptance and Usage of Technology [13], the Model of Adoption of Technology in Households [3], the Model of PC utilization [11], and the Innovation Diffusion Theory [9]. However, these MIS research models usually focus on technologies that promote positive outcomes and offer the user some sort of utility. However, computer security software is classified as a protective technology, which is strictly designed to avert negative outcomes and offers little obvious utility [5].

In an attempt to resolve the deficiency of MIS models for security adoption, a research model was constructed to examine the effectiveness of the constructs found in the Health Belief Model [10], a healthcare model from outside the information systems domain [4].

MODEL DEVELOPMENT

This work uses constructs and the survey instrument developed for the Security Adoption Behavior Model (SABM) [4] to explore the behaviors of home computer users in relation to the security measures taken on their computers using the research model shown in Figure 1. The slightly simplified conceptual model for the current work contains six core constructs that comprise Model 1 in the data analysis and results section below. The analysis also includes the interactions of the first five core constructs using prior experience with malware incidents as a moderator variable as Model 2. [4] assessed the overall quality of the model and found that it explained 30.4% of the variance in the home usage of computer security (adjusted R^2 was 0.167). For the current study, we used the factor analysis weighting of the survey instrument questions developed in [4] to measure each of these core constructs. This replication casts additional light on the complex issue of what induces individual users to mitigate risk of suffering a malware incident.

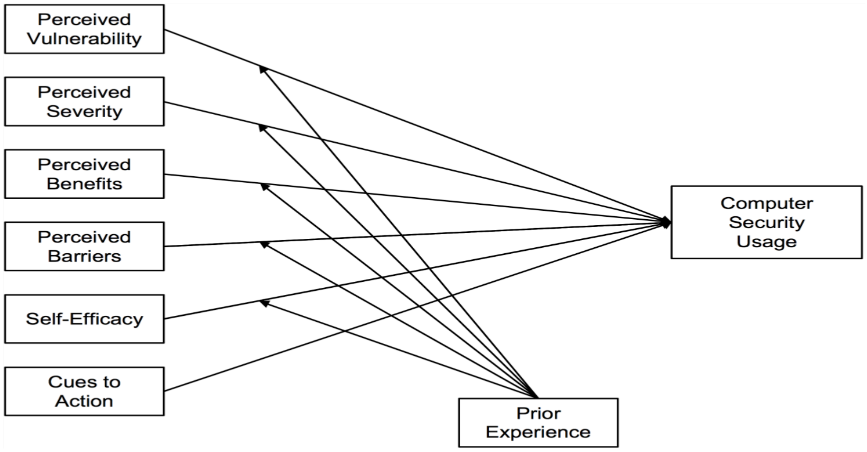

Figure 1. Research Model

Research Model Core Constructs

Brief explanations of the core and moderating constructs are presented with their associated research hypotheses. Tables 1 and 2 show the mapping of the survey instrument questions to each of the core constructs. Factor analysis weights were determined and validated in [4].

H1 – Perceived Vulnerability to security incidents is positively related to computer security usage. Perceived Vulnerability (VUL) is an individual's judgment of the security risk of his or her computer suffering from a particular security related issue.

H2 – Perceived severity of security incidents is positively related to computer security usage. Perceived Severity (SEV) is the individual's belief in the severity of the security compromise and its impact on lifestyle.

H3 – Perceived benefits of practicing computer security are positively related to computer security usage. Perceived Benefits (BEN) of an action is the belief in the effectiveness of the actions required to prevent a security risk

H4 - Perceived barriers of practicing computer security are negatively related to computer security usage. Perceived Barriers to Action (BAR) construct is the individual's belief in the benefits compared to the perceived costs of action. Perceived Barriers constitute obstacles to adoption and usage of security software for home computers.

H5 – Information Security Self-efficacy is positively related to computer security usage. Self-Efficacy (SEF) is an individual's belief in his or her own ability to carry out a particular task. For this study, it means the belief that the individual can install, configure, and maintain the security software on their computer.

H6 - Cues to action are positively related to computer security usage. Cues to Action (CUE): Even if a person is motivated and can perceive a beneficial action to take, actual change often occurs only in response to some external or internal cue.

Research Model Moderating Variable

Prior Experience (PXP)

H7a-e - Prior Experience (with security issues or attacks) significantly moderates the relationships of VUL, SEV, BEN, BAR and SEF on Computer Security Usage (CSU).

Research Model Dependent Variable

Computer Security Usage (CSU)

This is the dependent variable of the study as depicted in Figure 1. The measurement for this construct is self-reported usage of computer security software. It is assessed using questions to determine if the individual has anti-virus, firewall, and anti-spyware software installed and the level of usage. Software updates are not addressed in this study.

RESEARCH METHODOLOGY

Survey Design

This research used an Internet-based survey to test the proposed model. The survey used questions developed and presented in [4]. The population of interest is all Internet enabled computer owners that are at least partially responsible for the selection, installation, and maintenance of the software on their computers.

Perceived Vulnerability, Perceived Severity, and Perceived Benefits used the scenario based items listed in Table 1.- The questions for the remaining model constructs are listed in Table 2. All questions used a seven point scale.

Table 1 *Security Incident Scenarios and Core Construct Associations*

Scenario	Question (evaluated for likeliness, severity, and benefits)	Construct and Measure
1	My computer system becoming corrupted by a virus or worm.	**VUL1-8**: Highly Likely to Highly Un-Likely for vulnerability **SEV1-8**: Very important to not at all important for severity **BEN1-8**: Highly useful to not at all useful for benefits of using security software
2	My computer system being taken over by a hacker.	
3	My data corrupted by a virus or cyber-attack.	
4	My identity stolen (credit card number, Social Security Number, Bank account information, etc.).	
5	My data lost due to a virus or worm on my computer.	
6	The Internet becoming inaccessible because of computer security problems.	
7	Downloading a file that is infected with a virus through my e-mail.	
8	Downloading a file that is infected with a virus from the internet.	

Table 2 *Survey Question Items and Core Construct Associations*

Item	Question	Measure
BAR1	The expense of security software is a concern for me.	Highly Disagree to Highly Agree
BAR2	Using security software would change the way I use my computer.	Highly Disagree to Highly Agree
BAR3	Using security software effectively is time consuming.	Highly Disagree to Highly Agree
BAR4	Using security software is would require considerable investment of effort other than time.	Highly Disagree to Highly Agree
SEF1	I can select the appropriate security software for my home computer.	Not At All Confident to Totally Confident
SEF2	I can correctly install security software on my home computer(s).	Not At All Confident to Totally Confident
SEF3	I can correctly configure security software on my home computer(s).	Not At All Confident to Totally Confident
SEF4	I can find the information I need if I have problems using security software on my home computer(s).	Not At All Confident to Totally Confident
CUE1	If a friend were to tell me of a recent experience with a computer virus, I would be more conscious of my computer's chance of being attacked.	Highly Disagree to Highly Agree
CUE2	If my computer started behaving strangely, I would be concerned it had been the victim of a security attack.	Highly Disagree to Highly Agree
CUE3	If I saw a news report, or read a newspaper or magazine about a new computer vulnerability, I would be more concerned about my computer's chances of being attacked.	Highly Disagree to Highly Agree
CUE4	If I received an email from the maker of my computer’s operating system about a new security vulnerability, I would be more concerned about my computer's chances of being attacked.	Highly Disagree to Highly Agree
PXP1	How frequently have you been affected by a computer security problem?	Never to All the Time
PXP2	How recently have you been affected by a computer security problem?	Never to Within the Last Week
PXP3	The level of impact I have experienced from a computer security problem is:	Very Low/No Impact to Very High Impact
SSU1	I use add-on anti-virus software on my home computer(s).	Never to Always
SSU2	I use add-on firewall software on my home computer(s)	Never to Always
SSU3	I use add-on anti-spyware software on my home computer(s)	Never to Always

Data Collection

To recruit participants for the study members of undergraduate classes at a northwestern United States university were asked to complete the survey on SurveyMonkey.com. This website allows the survey to be filled out anonymously. Data collection yielded 99 usable surveys. Table 3 lists the sample participant characteristics.

Table 3: Sample Characteristics

Categorical Variable	**Frequency**	**Percent (%)**
Gender (GEN)		
Male	52	52.5
Female	45	45.4
No Answer	2	2.0
Operating System (OS)		
Windows XP or Earlier	2	2.0
Windows Vista	4	4.0
Windows 7	63	63.6
Windows 8	14	14.1
Apple OS X	14	14.1
Linux	2	2.0
Continuous Variable	**Value**	
AGE		
Mean	33.68	
Standard Deviation	11.75	

DATA ANALYSIS AND RESULTS

To test the hypotheses outlined above, a multiple regression analysis was conducted using SPSS with all non-dichotomous variables mean-centered prior to the regression analysis. The descriptive statistics for the variables used in the regression can be found in Table 4. The regression employed a hierarchical two-step method. In the first step (Model 1), the dependent variable Computer Security Usage was regressed on the six independent variables to determine main effects. The moderating variable: prior experience; and the hypothesized two-way interactions between it and the five independent variables comprised step two (Model 2). Regression results appear in Table 5.

This study supports the understanding that several individual human characteristics help explain individual adoption of security behavior and that there is still considerable room for improving this understanding and corresponding behavior.

Table 4 *Construct Descriptive Statistics*

Variable	Min	Max	Mean	St. Dev.	Skew	St. Err.	Kurtosis	St. Err.
Vulnerability	1.000	7.000	3.859	1.546	-0.011	0.243	-1.061	0.481
Severity	1.000	7.000	5.597	1.232	-1.254	0.243	1.881	0.481
Benefits	1.000	7.000	4.835	1.237	-0.897	0.243	0.956	0.481
Barriers	1.000	6.750	3.436	1.380	-0.057	0.243	-0.903	0.481
Cues to Action	1.000	7.000	5.000	1.086	-0.832	0.243	-1.358	0.481
Self Efficacy	1.500	7.000	5.760	1.329	-1.137	0.243	0.633	0.481
Prior Experience	1.000	5.000	2.394	0.907	0.272	0.243	-0.519	0.481
Computer Security Usage	1.000	7.000	5.027	2.066	-0.774	0.243	-0.603	0.481

In the current study, overall, the research model explains 35.3% of the variance in the dependent variable, computer security usage; slightly more than the 30.4% of the variance explained by the model as used in the prior study [4]. The main effects of vulnerability, severity, benefits, barriers, self-efficacy, and cues to action account for 26.2% of the explained variance, while the moderating variable, prior experience and the hypothesized two-way effects account for 9.1% of the variance in computer security usage.

In the Model 1 regression analysis, the core construct main effects of vulnerability, severity, benefits, barriers, self-efficacy, and cues to action, were tested (H1-H6). In model 2, the research hypotheses H7a-e were tested to determine the strength of the interaction effects of the moderating variable. In Table 5 the post-hoc t- test the number of asterisks next to each un-standardized coefficient indicates significance level for each model component.

Table 5: *Regression Results*

	Model 1 Coefficients	**Model 2 Coefficients**	**Result**
Vulnerability (VUL)	0.364**	0.297*	H1 Supported
Severity (SEV)	-0.364*	-0.315	H2 Not supported
Benefits (BEN)	0.273	0.264	H3 Not supported
Barriers (BAR)	-0.267	-0.315*	H4 Not supported
Self-Efficacy (SEF)	0.425**	0.372*	H5 Supported
Cues to Action (CUE)	0.351	0.254	H6 Not supported
Prior Experience (PXP)		0.089	
PXP * VUL		-0.110	H7a Not supported
PXP * SEV		0.454*	H7b Supported
PXP * BEN		-0.432*	H7c Supported
PXP * BAR		-0.040	H7d Not supported
PXP * SEF		0.221	H7e Not supported
	Model 1	**Model 2**	
R^2	0.262***	0.353***	
Adjusted R^2	0.214	0.263	
Change in R^2		0.091	

*p ≤ 0.05; **p ≤ 0.01; ***p ≤ 0.001

Model 1

In Model 1, the research hypotheses H1 through H6 were tested to determine the main effects of the Independent variables on the dependent variables. Results from the Model 1 analysis are listed in Table 5. Only two hypotheses were supported: H1 (vulnerability) and H5(self-efficacy) had significant coefficients as expected. Interestingly, the severity coefficient was significant but contrary to the hypothesis had a negative sign. This inconsistency may appear because a significant number of participants have a faulty or unrealistic perception of severity.

Model 2

The second model focused on research hypotheses H7a-e: that prior experience would have a significant moderating effect on the core constructs. As shown in Table 6, two hypotheses were supported: H7b and H7c. H7b with a coefficient showing significant moderating effect as hypothesized. Prior experience did interact with perceived benefits to produce a significant coefficient; however, unlike results in [4], it produced a negative coefficient. Please see the prior experience - perceived benefits interaction discussion that follows Figure 3 for a discussion of this results.

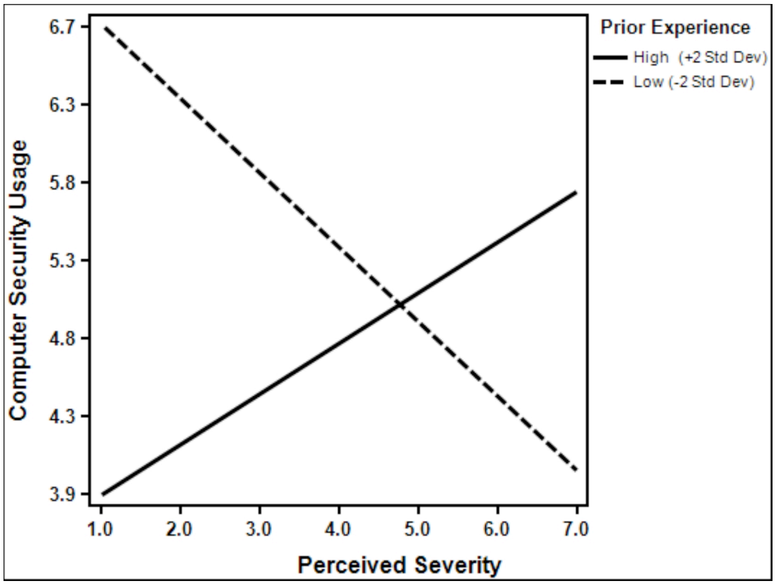

Figure 2. Interaction of Prior Experience and Perceived Severity

The interaction of prior experience and severity on computer security usage, Figure 2, shows that when prior experience with security incidents is high (+2 SD), perceived severity has a positive relationship with computer security usage. This is consistent with the hypothesis that perceived severity is positively related to computer security usage. However, when prior experience is low (-2 SD), the simple slope of the line takes on a negative value and the corresponding value of computer security decreases. This inconsistency may appear because participants with little prior experience have a faulty or very skewed perception of severity.

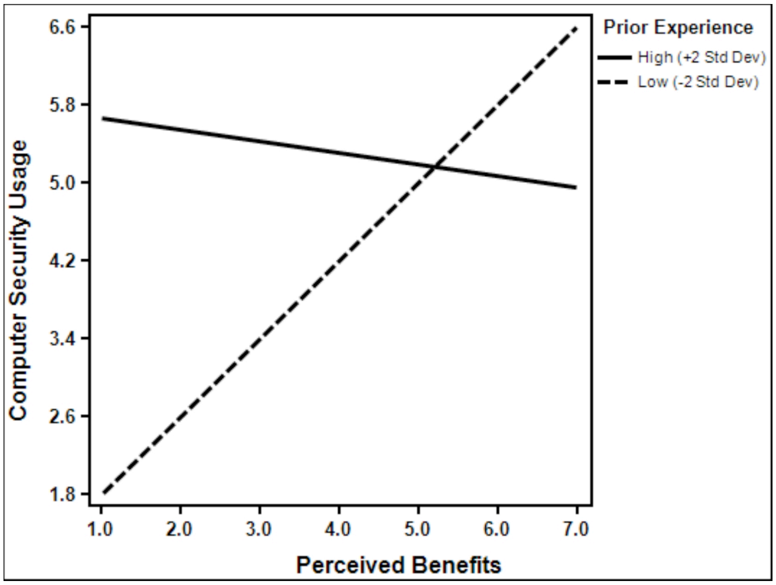

Figure 3. Interaction of Prior Experience and Perceived Benefits

The interaction of prior experience and perceived benefits on computer security usage, Figure 3, shows that when prior experience with security incidents is low (-2 SD), Perceived Benefits has a positive relationship with computer security usage. This is consistent with the hypothesis that perceived benefits is positively related to computer security usage. When prior experience is high (+2 SD) the relationship between Perceived Benefits and Computer Security Usage is slightly negative. This inconsistency may appear because participants with extensive prior malware events recognize that some problems can occur regardless of how diligently one behaves to mitigate risk. Another possible interpretation may be that students with prior malware experiences believe that mitigating security risks is not worth the expected benefit.

Respondents with low prior experience had a much more widely distributed range of perceived benefits and computer security usage. Those with high prior experience had a narrow range of computer security usage with a slightly negative slope to their perceived benefits. This unexpected distribution seems to be the key reason for the negative coefficient for this interaction.

CONCLUSIONS

The research model shown in Figure 1 presents 11 constructs and moderated interactions as predictors for computer security usage behavior in the home environment. This study provides empirical evidence that these constructs contribute to this understudied area of computer security. The results of this research also suggest that further evaluation of models based on the Health Belief Model may enhance the understanding of computer security adoption in the home.

Two of the constructs in the research model, perceived severity and cues to action, do not appear in other extant Information Systems models. While cues to action was not found to be a significant predictors of computer security usage in this research, it may still offer possible explanations of attitude that should be explored in the future.

The testing of the model with the current sample data revealed significant contributors to the usage of computer security were the perceived vulnerability of a security incident, perceived severity of security incidents and the moderating effect of prior experience with a security incident on perceived severity and perceived benefits of secure practices.

Implications for educators

The results presented above suggest that user education could influence users' perceptions of vulnerability and improve security software usage.

Limitations

One major limitation of this study is the non-random, college student-based sample used. The full population of interest (potentially all home computer users) is large and heterogeneous. The anonymous nature of the data collection and the sampling method lead to the possibility of non-responder bias which is impossible to measure in this study.

Another limitation is that the study used self-reported usage as a dependent variable. This could result in a self-report bias in which the respondents answer the usage measures in a way that would make their usage appear higher than would be measured through observation or experimentation. The results presented in [1] suggest that some home users hold unrealistic or inaccurate views of the vulnerability and level of risk mitigation on their home computers.

The use of an online survey limits the respondent pool to those that felt comfortable completing the survey, creating a potential response bias.

Future Research

An obvious addition to this study would be a replication using different samples from the target population, such as international samples. Another option would be to combine the most significant constructs from this model with those from another effective tool such as the Unified Theory of Acceptance and Use of Technology (UTAUT) described in [13].

This study considered computer security usage as the application of anti-virus, firewall, and anti-spyware software. Future applications of the model could be extended to the behaviors involved in opening suspicious emails, using suspicious websites, file sharing, and other high-risk online activities.

Finally, the application of the HBM to the study of security adoption can be extended beyond the home environment to study security adoption behavior in the corporate environment.

REFERENCES

[1] AOL and National Cyber Security Alliance (NCSA), (2005). AOL/NCSA Online Safety Study.

[2] Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes, 50*, 179-211.

[3] Brown, S.A., Venkatesh, V. (2005). Model of Adoption of Technology in Households: A Baseline Model Test and Extension Incorporating Household Life Cycle, *MIS Quarterly, 29*(3), 399-426

[4] Claar, C., & Johnson, J. (2012). Analyzing home PC security adoption behavior*. Journal of Computer Information Systems, Summer 2012, 20-29.*

[5] Conklin, Wm. Arthur (2006). Computer security behaviors of home PC users: A diffusion of innovation approach. Ph.D. dissertation, The University of Texas at San Antonio, United States -- Texas. Retrieved September 27, 2009, from Dissertations & Theses: Full Text.(Publication No. AAT 3227760).

[6] *Consumer Reports*. (2013) Meanwhile, on your home computer…, June 2013, 21.

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

[8] Fishbein, M. & Ajzen, I. (1975). Belief, Attitude, Intention, and Behavior: An Introduction to Theory and Research. Boston: Addison-Wesley.

[9] Rogers, E.M., *Diffusion of Innovations*. Fifth ed. 2003, New York, New York, U.S.A.: The Free Press.

[10] Rosenstock I., Strecher, V., & Becker, M. (1994). The Health Belief Model and HIV risk behavior change. In R.J. DiClemente & J.L. Peterson (Eds.), *Preventing AIDS: Theories and methods of behavioral interventions* (pp. 5-24). New York, NY: Plenum Press.

[11] Thompson, R. L., Higgins, C. A., & Howell, J. M. (1991). Personal computing: Toward a conceptual model of utilization. *MIS Quarterly, 15(*1), 131.

[12] U.S. Census Bureau, (2012), Computer and Internet Use in the United States: 2010, downloaded 2 May 2012 from http://www.census.gov/hhes/computer/publications/2010.html

[13] Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly, 27(*3), 425-478.

Acknowledgements: We want to thank the anonymous reviewers for their suggestions to improve the clarity of this work.