Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 2012 Proceedings | Proceedings

Browser Update Practices in Households: Insights from Protection Motivation Theory and Customer Satisfaction

Srikar Velichety
Management Information Systems, University of Arizona, Tucson, AZ, United States., srikarv@email.arizona.edu

Alexandra Durcikova
The University of Arizona, Tucson, United States., alex@eller.arizona.edu

Follow this and additional works at: http://aisel.aisnet.org/amcis2012

Recommended Citation
Velichety, Srikar and Durcikova, Alexandra, "Browser Update Practices in Households: Insights from Protection Motivation Theory and Customer Satisfaction" (2012). *AMCIS 2012 Proceedings*. 18.
http://aisel.aisnet.org/amcis2012/proceedings/ISSecurity/18

This material is brought to you by the Americas Conference on Information Systems (AMCIS) at AIS Electronic Library (AISeL). It has been accepted for inclusion in AMCIS 2012 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.

Browser Update Practices in Households: Insights from Protection Motivation Theory and Customer Satisfaction

Research-in-Progress

Srikar Velichety
University of Arizona
srikarv@email.arizona.edu

Alexandra Durcikova
University of Arizona
alex@eller.arizona.edu

ABSTRACT

Web Browser is the most common tool used for surfing the Internet. With personal computer users growing by leaps and bounds, the use of browsers is also increasing at a similar rate. Outdated versions of browsers have security flaws and hence represent a significant threat to the cyber infrastructure. Yet many users do not keep their browsers updated. Given the fact that voluntariness of action characterizes personal computer users' security behavior, we argue that satisfaction derived from using the browser along with perceptions of threat severity and vulnerability play an important role in browser update intention. However, considering the inconsistency of household computer users' behavior, we posit that urgency plays a role in the browser update behavior. Using a combined model of Customer Satisfaction and Protection Motivation Theory along with positive and negative urgency as direct antecedents' to behavior, we evaluate the important antecedents to browser update intentions.

Keywords

Information Security, Personal Computer User Security, Browsers, Updates, Customer Satisfaction, Impulsiveness, Urgency Protection Motivation Theory.

INTRODUCTION

The two most common services used on the Internet are Email and Web (Smith, 2010). The number of personal computer users who use these two services surpassed 1 billion in 2008 and is expected to double by 2014 (Pettey and Stevens, 2010). The ever increasing speed of home Internet connection with the high number of security vulnerabilities associated with outdated versions of browser or email clients (Reis, Barth and Pizano, 2009) present a significant security threat to the cyber infrastructure (Anderson and Agarwal, 2010). Computers that haven't been properly patched can be easy targets of hackers who can then either steel personal information of the computer owner or install malware and use the computer in a Distributed Denial of Service Attack (Milletary, 2005). While vendors are providing automatic updates (Reis et al., 2009), by modifying the architecture of the browsers to provide safe browsing and by updating the list of phishing sites regularly (Reis et al., 2009), it is up to the user to install the updates or to install the new version of the software that is more secure. In short technology cannot alone solve all the problems associated with using the outdated versions of the browsers; end users play an integral role. This underscores the need for research on the motivation factors behind personal computer users' security behaviors.

LITERATURE REVIEW

A large part of behavioral information security research has concentrated on firms where the management can use coercive methods on employees for failing to follow the information security policies (Li and Siponen, 2011). While Boss et al., (2009) used the elements of control theory to explain the perception levels of mandatoriness of information security policies, Bulgurcu et al ., (2010) combined elements of the Theory of Planned Behavior and Rational Choice Theory with information security awareness to postulate that the belief of the overall assessment of consequences of an employee are shaped by the outcome beliefs concerning events that follow compliance or non-compliance. While we find significant research on decision to upgrade software in the context of an organization (Huoy and Robey, 2007) and on technology adoption in households (Brown and Venkatesh, 2005), the security component of household computer updates is missing. No reported research in the literature so far has used a theoretical model to determine the important factors behind personal computer user's browser

update intentions even though these users represent 77.3% of all the users (United States Internet Usage, Broadband and Telecommunications Reports - Statistics, 2010).

Personal computer user security has remained a passive area in the information security research community (Li and Siponen, 2011). This was partly due to the fact that reported incidents of security breaches and information losses in organizations attracted more attention. Most of the previous research reported in this area has concentrated on extending the existing theories in the organizational context by adding new constructs that were believed to influence household computer use (Ng and Rahim, 2005; Woon, Tan and Low, 2005; Lee and Kozar, 2008). In doing so, it failed to consider the multitude of differences that exist in a home and work environment (Li and Siponen, 2011) such as lack of information technology support, voluntariness in following security policies and absence of monitoring mechanisms.

CONTEXT OF HOME USER SECURITY

Browsers are used for a variety of personal purposes including internet banking, online shopping, gaming, or email., where users store their personal and sensitive information (e.g., username and password) which if compromised could not only cause damage to them but also to the companies that host the websites. Li and Siponen (2011) claim that an attack on personal computer users could be the breeding ground for a larger attack on the organizations. Apart from these, malware and spyware are known to propagate primarily through outdated browsers (Wadlow and Gorelik, 2009) thus further increasing the risk of security breach on household computers.

Browser is the most appealing target to attackers considering its trusted computing base with a large internet population (Reis et al., 2009). Vendors, taking cognizance of this fact, deploy a multitude of resources into fixing the security flaws in the present versions. However, it is up to the user to update the browser or not. In an organizational context, companies can use coercive methods against employees who fail to follow security policies (Ng and Rahim, 2005). Moreover, they invest heavily to make sure that the systems are safe by employing information security personnel who are charged with the responsibility of overseeing all the security related activities including system and software updates (Li and Siponen, 2011). In a home environment, the assurance for security is missing (Li and Siponen, 2011). Vendors also admit that designing a browser that is just suitable for a user is impossible considering the evolving security threats (Wadlow and Gorelik, 2009). Considering the vulnerabilities mentioned here and the limitations of technology in dealing with them, it is important to understand the various factors behind personal computer user's intention to update the browsers. We step up to this need by supplementing Protection Motivation Theory (PMT) with Customer Satisfaction and Urgency. Just as the class of models on information security assume, we posit that intention directly affects behavior (Venkatesh, Morris and Davis, 2003). However, in order to account for the inconsistencies in behavior, we use positive and negative urgency as direct determinants to behavior.

PROTECTION MOTIVATION THEORY

Protection Motivation Theory (PMT) was initially created to clarify the effect of fear appeals on intent to change behavior in healthcare (Rogers, 1975). Fear appeals are persuasive messages designed to scare people by describing what could happen to them if they do not follow the recommended behavior (Witte, 1992). Severity of threat, individual's susceptibility to threat, and statements of efficacy in terms of recommended response and the ability to perform recommended response considering the cost incurred for the same form the essential elements of fear appeal (Johnston and Warkentin, 2010).

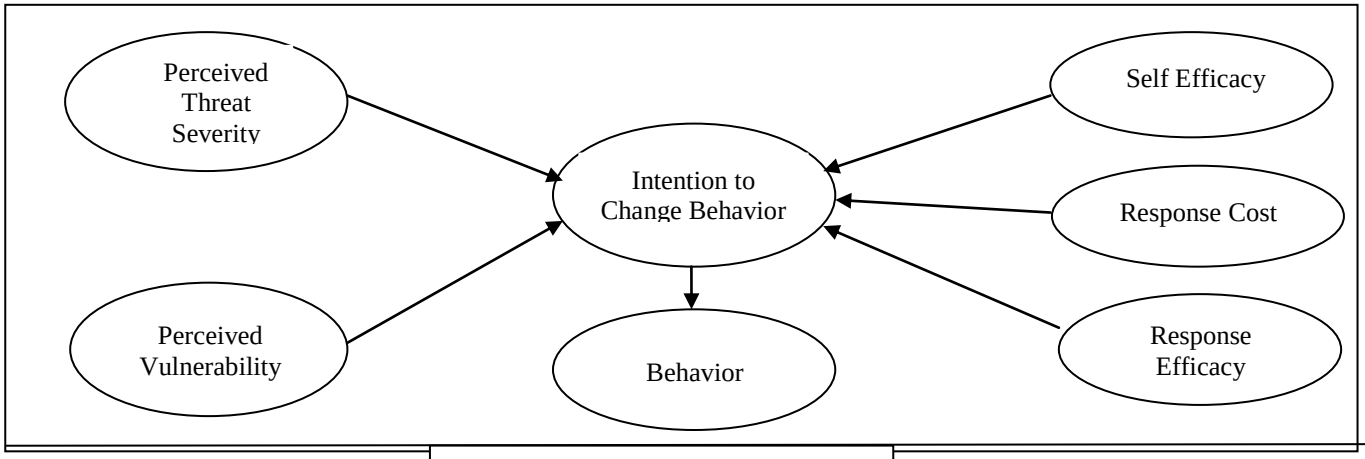

Figure 2 - Protection Motivation Theory

PMT was combined with various other theories to study the security behavior of employees in an organizational context. While Johnston and Warkentin (2010) used PMT embedded with social influence factor to evaluate the efficiency of fear appeals, Ng et al., (2009) and Herath and Rao (2009) combined PMT with health-belief model and deterrence model respectively to study the intentions behind security policy compliance. Their results show that perceived threat severity significantly affects the concern regarding security breaches and that perceived susceptibility and self-efficacy are major determinants in the context of e-mail attachments. Johnston and Warkentin (2010) also found that response efficacy and self efficacy have a positive influence on the end users' intention to comply with security policies.

PMT was also used to study the security behavior of personal computer users. While Woon et al., (2005) found that perceived threat severity, response efficacy, self- efficacy and response cost are the major determinants that affect the decision of home wireless users to implement security features in their networks, LaRose et al., (2005) found that efficacy of the available software protections and efficiency in implementing those protections were the important determinants of online safety behavior. All these results show that the elements of PMT play a significant role in personal computer users' intention to practice security. We hence use this to evaluate the effect of fear appeals on household browser update intentions and actual update behavior.

Perceived Threat Severity

Perceived threat severity is the assessment of the damage caused by a particular threat (Milne, Sheeran and Orbel, 2000). The first thing that should be considered in the context of a household browser update intention is whether the user perceives surfing the internet with an outdated version of the browser as a security threat at all. Health-belief model asserts that a user's perceived threat severity positively influences security compliance in an organizational context (Ng et al., 2009). Woon et al., (2005) found that perceived threat severity is one of the key determinants of home users' intention to practice security on wireless networks. We posit that when home users consider outdated versions of browsers as a security threat they will react positively to the browser updates.

> H1: Perceived threat severity of the outdated version of the browser has a positive effect on a home user's intent to update a browser.

Perceived Vulnerability

Perceived vulnerability refers to a persons' assessment of his/her own probability of being exposed to the threat (Rogers, 1983). In the context of a browser update, this can be interpreted in terms of a user's assessment of the probability of being subjected to a virus or hacking attack because of an outdated version of a browser. While personal computer users to a large extent are known to put perceived utility over security while browsing (Reis et al 2009), assessment of the threats confronted by an outdated browser could positively influence their intention to update the browser. Thus we hypothesize that:

H2: Perceived vulnerability of the security threat from an outdated browser will have a positive effect on a home user's intent to update a browser.

Self-Efficacy

Self efficacy is defined as the expectancy of a person's capability in performing a recommended coping behavior, in this case updating the browser (Bandura, 1977). In studies based on self-efficacy theory (Bandura, 1977), self-efficacy has been found to have a significant positive effect on behavioral change (Bandura, Adams, Hardy and Howells, 1980; Condiotte and Lichtenstein, 1981; Woon et al., 2005). A quantitative study by Milne et al., (2000) has shown that among all PMT independent variables, self-efficacy has the most robust effect on intention. Hence we hypothesize that:

> H3: Self-Efficacy of updating the browser has a positive effect on the home users' intention to update a browser.

Response Efficacy

Response Efficacy is the belief that the recommended security measure will be effective in protecting from security threats (Bandura, 1977). Past studies (Maddux and Stanley, 1986; Wurtele, 1988) have shown that there is a positive relationship between response efficacy and coping response. Woon et al., (2005) found that response efficacy plays and important role in home user's intention to practice security on wireless networks. Hence we hypothesize that:

H4: Response efficacy of the updated version of the browser in preventing security threats will positively influence home user's intention to update a browser.

Response Cost

Response cost is the belief about the cost associated with performing a coping behavior (Rogers, 1983). The cost in this case may include inconvenience, difficulty and other repercussions of updating browsers. A Survey by Mozilla Software foundation (Metrics, 2010) about the reasons behind not updating browsers had many people report that updates in the past have caused crashes, speed or memory leaks and dysfunctional add-ons. Reis et al., (2009) assert that personal computer users do not update their browsers when they realize that the required functionalities do not work on the updated versions. Therefore we hypothesize that:

H5: Response Costs associated with browser updates will have a negative effect on the personal computer user's intention to update a browser.

Finally, as a replication of past literature showing that behavioral intention strongly influences behavior (e.g., Venkatesh et al., 2003), we also predict that behavioral intention to upgrade a browser will influence personal computer users' actual upgrading behavior. Hence, we predict:

H6. An increase in browser update intention will increase secure behavior.

CUSTOMER SATISFACTION

Customer Satisfaction is defined as the percentage of total customers whose reported experience with a firm, its products, or its services exceeds specified satisfaction goals (Farris, Bendle, Pfeifer, & Reibstein, 2010). Customer satisfaction with software products has been widely studied by MIS researchers. Kekre et al., (1995) analyzed customer satisfaction for eight different IBM products and found that capability and usability are the dominant factors, followed closely by the performance factor. Krishnan and Ramaswamy (1998), in a survey of intranet marketing systems found that features that lower the cost of ownership and provide competitive benefits were the important drivers of customer satisfaction. Krishnan and Subramanyam (2004) found that usability dominates other satisfaction factors for North American customers in the case e-commerce software. In a study similar to this one, Susarla et al., (2003) used consumer satisfaction paradigm from marketing literature to analyze the post-usage satisfaction with application service providers. They found that expectations about the service have a significant influence on the performance evaluation while experience-based norms have only a limited influence.

Browser updates happen at a fast pace. For example, Microsoft's Internet Explorer went from IE 1.0 to IE 6.0 with 19 releases in 6 years, its main rival Netscape Navigator went through 28 versions in 7 years (blooberry.com, 2011). While vendors constantly change browsers at this pace to make them more powerful and overcome the existing security flaws, some existing users may be annoyed by the rate of change or some minor difference in the way they have to use the updated products (Wang and Butler, 2003). A Survey by Mozilla Software foundation on the reasons behind not updating the browsers found that typically 57% of the respondents were happy with the existing version (Metrics, 2010) and hence opted out for upgrade. Hence we argue that once the customer realizes that the updated versions of the browser offers a little utility over the present one with which he is satisfied, he will react negatively to the browser updates. Therefore we hypothesize that

H7: Customer Satisfaction has a negative effect on household computer user's intent to update a browser.

Urgency

According to marketing literature, urgency occurs when consumers experience a sudden powerful urge to buy something immediately with diminished regard to consequences (Rook, 1987). Cyders and Smith (2008) categorized these urges as positive and negative referring to the individual disposition to engage in impulsive action when experiencing extreme positive and negative affect, respectively. Psychology research suggests that individuals can have multiple attitudes towards the same object and that the most temporarily valued or accessible attitudes dominate (Wood, 2000). Home computer user behavior is more uncertain and inconsistent when compared to the behavior of individuals at work place (Li and Siponen, 2011). We posit that this inconsistency could possibly be a result of people deciding to either click on not click on the update notifications because of the state they are in. This state could in turn be the result of people reacting emotionally to computers (Ball & Breese, 1999) which could make them either angry or joyful .Therefore we argue here that urgency plays an important role in browser update behavior and can possibly overshadow the elements of careful forethought i.e., the antecedents to browser update intention. Hence we hypothesize:

H8: Positive urgency has a positive effect on a personal computer user's behavior of updating a browser.

H9: Negative urgency has a Negative effect on a personal computer user's behavior of updating a browser.

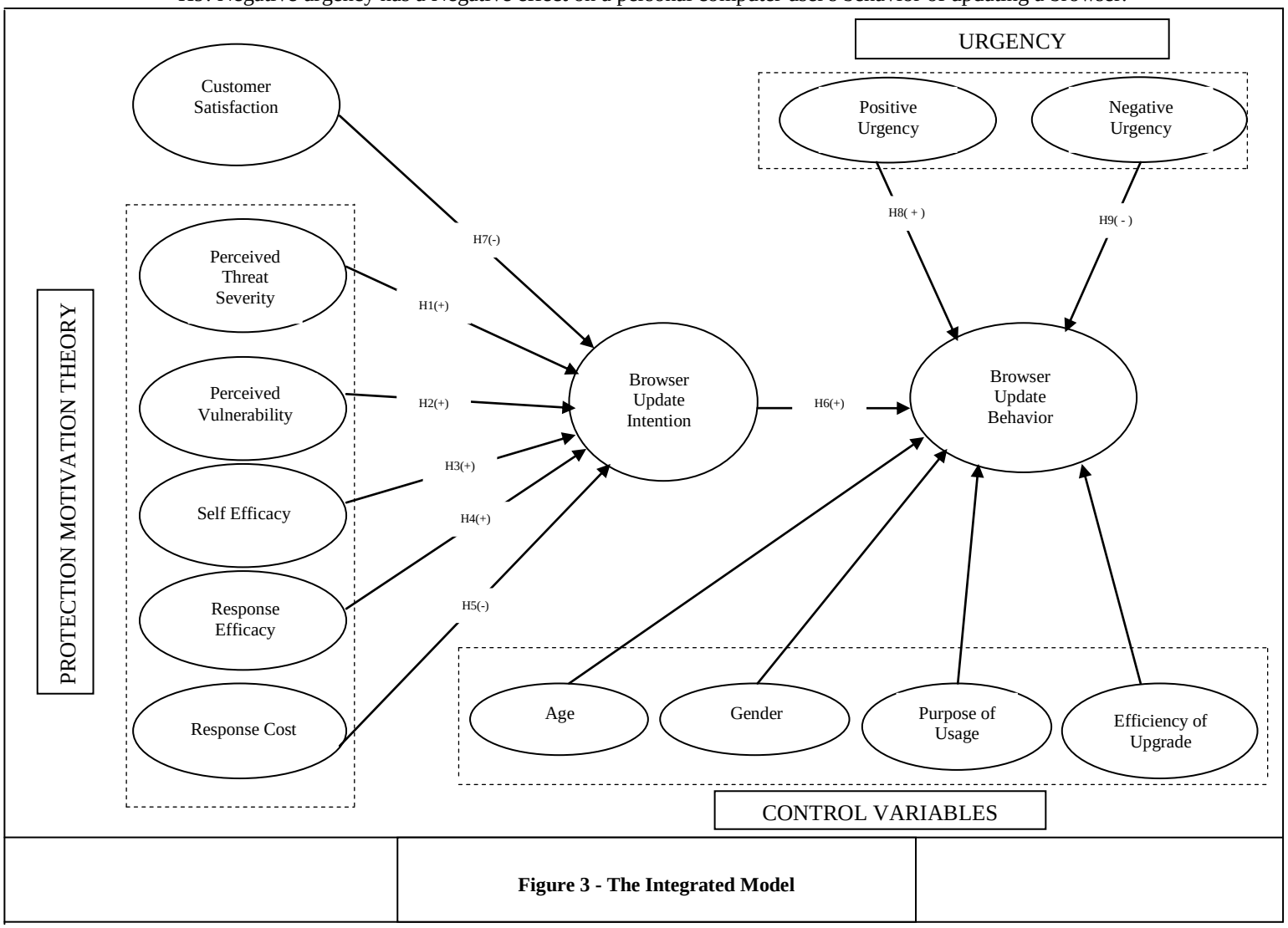

Figure 3 - The Integrated Model

CONTROL VARIABLES

The model showing all the constructs and hypothesized relationships is depicted in Figure 3. In order to account for the effect of extraneous factors that have been shown in past research to influence browser update behavior or IS use behavior, we included age, gender, purpose of usage and efficiency of upgrade as the control variables. Literature also suggests that a person's age plays an important role in willingness to accept a change in a new technology with younger users more willing to do so (Morris and Venkatesh, 2000) . Hence we need to control for the age of the population in the survey. Also a study of the technology usage of 342 workers (Venkatesh and Morris, 2000) found that the technology usage decisions of men are strongly influenced by perceptions of usefulness and those of women were influenced by perceived ease of use and subjective norm. Women also tend to find software less easy to use than men (Gefen and Straub, 1997) and have greater computer anxiety (Igbaria and Chakrabarti, 1990; Whitley and others, 1997). When employees use their computers at home for the purpose of office related work, they are mandated to keep the software updated on the machines (Li and Siponen, 2011) and hence we need to control for the purpose of usage. A Survey by Mozilla Software foundation in 2009 on the reasons for not upgrading had 25% report that it was due to crashes or trouble in updating (Metrics, 2010). Hence it is reasonable to state that the efficiency of upgrade will have an effect on the browser update behavior.

METHODOLOGY

To test the hypothesized relationships, a questionnaire addressing all constructs will be administered through an online survey. Customer Satisfaction is adapted from Doll and Torkzadeh (1988), perceived threat severity, perceived vulnerability, self-efficacy, response efficacy and response cost adapted from Woon et al (2005) and positive and negative urgency from Cyders et al., (2007) and Whitside and Lynam (2001) respectively. All the items will be measure using a 5 point Likert scale: from 1 ("Strongly Disagree") to 5 ("Strongly Agree"). Table 1 shows the descriptions of the items used for measuring the constructs. Subjects of this research are home computer users ages 18 and up that use both PC and Mac computers and use any browser when surfing the Internet. The subjects will also be provided with a dictionary of terms used in the survey like hacking, plugins, malware etc., The proposed model will be tested using SEM.

Construct	ITEM		Source
Customer Satisfaction		"My browser …	
	CustSat1	provides the precise information needed from web pages	Doll and Torkzadeh (1988)
	CustSat2	has features that meet my browsing needs	
	CustSat3	presents the information in the webpages in just about exactly the way I need	
	CustSat4	provides sufficient information about the web pages	
	CustSat5	is accurate in terms of functioning of the plugins	
	CustSat6	provides satisfactory accuracy	
	CustSat7	presents the information on the web page in correct format	
	CustSat8	provides the information clearly	
	CustSat9	is user friendly	
	CustSat10	is easy to use	
	CustSat11	gives the information needed in time	
	CustSat12	provides compatibility for the required plugins	
Perceived Threat Severity	PThreatSev1	Having my online identity stolen as a result of hacking through a security flaw in an outdate browser is a serious problem to me	Woon et al., (2005)
	PThreatSev2	Having my computer infected as a result of viruses and malware spreading through outdated browsers is a serious problem to me.	
	PThreatSev3	Losing my confidential information like online banking account login details and credit card no as a result of outdated browser is a serious problem to me.	
	PThreatSev4	Loss resulting from outdated version of browsers is not a serious problem to me.	
Perceived Vulnerability	PerVul1	I could be subject to a malicious attack as a result of outdated browser.	Woon et al., (2005)

	PerVul2	I feel that I am vulnerable to hacking through browser.	
	PerVul3	I feel that my computer would be at risk because of an outdated version of a browser.	
Self Efficacy	SelEff1	It is easy for me to update the browser by myself	Woon et al., (2005)
	SelEff2	I can update the browser even if there is no one around me to tell me what to do	
	SelfEff3	I can update my browser only if I have a reference manual to do so.	
Response Efficacy	ResEff1	Keeping my browser updated is an important step in deterring hackers from attacks.	Woon et al., (2005)
	ResEff2	Keeping my browser updated will prevent hackers from breaking into my computer and stealing personal information	
	ResEff3	Keeping my browser updated will help me protect my computer from viruses	
Response Cost	ResCost1	Updating my browser requires a considerable investment in Time	Woon et al., (2005)
	ResCost2	There are too many overheads associated with updating my browser	
	ResCost3	Updating my browser requires a considerable effort other than time	
	ResCost4	Updating my browser causes problems like memory leaks, dysfunctional add-ons and crashes	
Positive Urgency	PosUrg1	When I am very happy, I can't seem to stop myself from doing things that can have bad consequences.	Cyders et al., (2007)
	PosUrg2	When I am in great mood, I tend to get into situations that could cause me problems.	
	PosUrg3	When I am very happy, I tend to do things that may cause problems in my life.	
	PosUrg4	I tend to lose control when I am in a great mood.	
	PosUrg5	When I am really ecstatic, I tend to get out of control.	
	PosUrg6	Others would say I make bad choices when I am extremely happy about something.	
	PosUrg7	Others are shocked or worried about the things I do when I am feeling very excited.	
	PosUrg8	When I get really happy about something, I tend to do things that can have bad consequences.	
	PosUrg9	When overjoyed, I feel like I can't stop myself from going overboard.	
	PosUrg10	When I am really excited, I tend not to think of the consequences of my actions.	
	PosUrg11	I tend to act without thinking when I am really excited.	

	PosUrg12	When I am really happy, I often find myself in situations that I normally wouldn't be comfortable with	
	PosUrg13	When I am very happy, I feel like it is OK to give in to cravings or overindulge.	
	PosUrg14	I am surprised at the things I do while in a great mood.	
Negative Urgency	NegUrg1	I have trouble controlling my impulses.	Whitside and Lynam (2010)
	NegUrg2	I have trouble resisting my cravings (for food, cigarettes, etc.).	
	NegUrg3	I often get involved in things I later wish I could get out of.	
	NegUrg4	When I feel bad, I will often do things I later regret in order to make myself feel better now.	
	NegUrg5	Sometimes when I feel bad, I can't seem to stop what I am doing even though it is making me feel worse.	
	NegUrg6	When I am upset I often act without thinking.	
	NegUrg7	When I feel rejected, I will often say things that I later regret.	
	NegUrg8	It is hard for me to resist acting on my feelings.	
	NegUrg9	I often make matters worse because I act without thinking when I am upset.	
	NegUrg10	In the heat of an argument, I will often say things that I later regret.	
	NegUrg11	I am always able to keep my feelings under control.	
	NegUrg12	Sometimes I do things on impulse that I later regret	
Efficiency of Upgrade		I could successfully upgrade my browser ...	Mozilla Software Foundation (Metrics, 2010)
	EffUpgrd1	If I do not expect to experience crashes during the process.	
	EffUpgrd2	If I do not have trouble with upgrading.	
	EffUpgrd3	If it doesn't take a lot of time.	

Table 1 - Items for the Constructs

CONCLUSION

This study proposes a model that studies household users' browser update behavior. This study extends PMT by including two important concepts from marketing literature, namely, customer satisfaction and impulsiveness. We propose to study browser update behavior on home computers because these end users are not required to follow any security policy, yet due to ever increasing speeds of home Internet access they are becoming targets of hackers who can either exploit their private information or use the vulnerable computer in DDOS.

REFERENCES

1. Anderson, C. L. and Agarwal, R. (2010). Practicing Safe Computing - A Multimethod Empirical Examination of Home Computer User Security Behavioral Intentions. *MIS Quarterly , 34* (3),613-624.
2. Ball, G., and Breese, J. (1999). Modeling the emotional state of computer users. Workshop on'Attitude, Personality and Emotions in User-Adapted Interaction', UM'99.

3. Bandura, A. (1977). Self - efficacy: Toward a unifying theory of behavioral change. *Psychological Review, 84,*191-215.
4. Bandura, A., Adams, N., Hardy, A. and Howells, G. (1980). Tests of the Generality of Self Efficacy Theory. *Cognitive Therapy and Research, 4*, 39-66.
5. blooberry.com,2011.Browser History: Windows Internet Explorer, http://blooberry.com/indexdot/history/ie.htm
6. Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A. and Boss, R. W. (2009). If Someone is Watching I'll do what I am asked : mandatoriness, control and information security. *European Journal of Information Systems , 18*, 151-164.
7. Brown, S. A. and Venkatesh, V. (2005). Model of Adoption of Technology in Households : A Baseline Model Test and Extension. *MIS Quarterly , 29* (3), 399-426.
8. Bulgurcu, B., Cavusoglu, H. and Benbasat, I. (2010). Information Security Policy Compliance - An Empirical Study of Rationality Based Beliefs and Information Security Awareness. *MIS Quarterly , 34* (3), 523-548.
9. Condiotte, M. M. and Lichtenstein, E. (1981). Self Efficacy and Relapse in Smoking Cessation Programs. *Journal of Consulting and Clinical Psychology, 49*, 648–658.
10. Cyders, A.M.,Smith G.T.,Spillane N.S.,Fischer S.,Annus M.A. & Peterson C.(2007). Integration of Impulsivity and positive mood to predict risky behavior : Development and validation of a measure of positive urgency. *Psychological Assessment, 19(1),* 107-118.
11. Cyders, M.A. and Smith, G.T. (2008). Emotion Based Dispositions to Rash Action : Positive and Negative Urgency. *Psychological Bulletin, 134(6),* 807-828.
12. Dinev, T. and Hu, Q. (2007). The Centrality Awareness in the formation of user behavioral intent towards protective information technologies. *Journal of the Association of Information Systems , 8 (7),* 386-408.
13. Doll,W.J. and Torkzaedeh, G.(1988). The Measurement of End-User Computing Satisfaction. *MIS Quarterly, 12(2),* 259-274.
14. Farris, P., Bendle, N. T., Pfeifer, P. E., & Reibstein, D. J. (2010). *Marketing Metrics: The definitive guide to measuring marketing performance*. Wharton.
15. Herath, T. and Rao, H.R. (2009). Protection Motivation and Deterrence : a framework for security policy compliance in organisations. *European Journal of Information Systems, 18,* 106-125.
16. Huoy, M. K. and Robey, D. (2007). Deciding to Upgrade Packaged Software - a comparative case study of motives, contingencies and dependencies. *European Journal of Information Systems , 16*, 555-567.
17. Igbaria, M. and Chakrabarti, A. (1990). Computer anxiety and attitudes towards microcomputer use. *Behaviour & Information Technology*, *9*(3), 229–241.
18. Johnston, A.C. and Warkentin, M. (2010). Fear Appeals and Information Security Behaviors : An Empirical Study. *MIS Quarterly, 34(3),* 549-566.
19. Krishnan, M. and Subramanyam, R. (2004). Quality dimensions in e-commerce software tools: an empirical analysis of North American and Japanese markets. *Journal of Organizational Computing and Electronic Commerce*, *14*(4), 223–241.
20. Krishnan, M. S. (1993). Cost, quality and user satisfaction of software products: an empirical analysis. Proceedings of the 1993 conference of the Centre for Advanced Studies on Collaborative research: software engineering-Volume 1 (pp. 400–411).
21. Krishnan, M. S. and Ramaswamy, V. (1998). An empirical analysis of customer satisfaction for Intranet marketing systems. *Decision Support Systems*, *24*(1), 45–54.
22. Kristensen, K., Martensen, A. and Gronhold, L. (2000). Customer satisfaction measurement at Post Denmark : Results of application of the European Customer Satisfaction Index Methodology. *Total Quality Management, 11(7),* 1007-1015.
23. LaRose, R., Rifon, N., Liu, S., & Lee, D. (2005). Understanding online safety behavior: A multivariate model. *The 55th Annual Conference of the International Communication Association, New York City*.
24. Lee, Y. and Kozar, K. (2008). An Empirical Investigation of anti-spyware software adoption : A multitheoritical perspective. *Information & Management , 45* (2), 109-119.
25. Li, Y. and Siponen, M. (2011). A Call For Research on Home Users' Information Security Behavior. *15th Pacific Asia Conference on Information Systems (PACIS).* Brisbane, Australia.

26. Maddux, J. E. and Rogers, R. W (1983). Protection Motivation Theory and Self Efficacy: A Revised Theory of Fear Appeals and Attitude Change. *Journal of Experimental Social Psychology, 19*, 469-479.
27. Metrics, B. o. (2010, April 21). *Why People Don't Upgrade Their Browser - Part IV*. Retrieved January 18, 2012, from The Mozilla Blog: http://blog.mozilla.com/metrics/2010/04/21/why-people-don%E2%80%99t-upgrade-their-browser-%E2%80%93-part-iv/.
28. Milletary, J. (2005). Technical Trends in Phishing Attacks. US-CERT.
29. Milne, S., Sheeran, P. and Orbell, S. (2000). Prediction and Intervention in Health-related Behavior: A Meta-analytic of Protection Motivation Theory. *Journal of Applied Social Psychology, 30(1)*, 106-143.
30. Morris, M. G. and Venkatesh, V. (2000). Age differences in technology adoption decisions: Implications for a changing work force. *Personnel psychology*, *53*(2), 375–403.
31. Ng, B. -Y. and Rahim, M. (2005). A Socio-Behavioral study of home computer users intention to practice security. *PACIS.* Las Vegas Nevada.
32. Ng, B.Y. , Kankanhalli, A. and Xu, C. (2009). Studying users' computer security behavior : A health belief perspective, *Decision Support Systems, 46*, 815-825.
33. Pettey, Christy, and Holly Stevens. *Gartner Highlights Key Predictions for IT Organizations and Users in 2010 and Beyon.* January 13, 2010. http://www.gartner.com/it/page.jsp?id=1278413 (accessed January 12, 2012).
34. Reis, C., Barth, A. and Pizano, C. (2009). Browser Security : Lessons from Google Chrome. *Communications of the ACM , 52 (8)*, 45-49.
35. Rogers, R. W. (1975). A Protection Motivation Theory of Fear Appeals and Attitude Change1. *The Journal of Psychology*, *91*(1), 93–114.
36. Rogers, R. W. (1983). Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. *Social psychophysiology*, 153–176.
37. Rook, R.W. (1987). The Buying Impulse. *Journal of Consumer Research, 14(2)*, 189-199.
38. Smith, C. (2010, 06 22). Internet Usage Statistics : How We Spend Our Time Online (INFOGRAPHIC). Retrieved 02 17, 2012, from Huffington Post: http://www.huffingtonpost.com/2010/06/22/internet-usage-statistics_n_620946.html.
39. Susarla, A., Barua, A. and Whinston, A. B. (2003). Understanding the service component of application service provision: empirical analysis of satisfaction with ASP services. *MIS Quarterly*, *27*(1), 91–123.
40. *United States Internet Usage, Broadband and Telecommunications Reports - Statistics*. (2010, 06). Retrieved 02 25, 2012, from Internet World Stats: http://www.internetworldstats.com/am/us.htm.
41. Venkatesh, V. and Morris, M. G. (2000). Why don't men ever stop to ask for directions? Gender, social influence, and their role in technology acceptance and usage behavior. *MIS Quarterly*, *24(1)*, 115–139.
42. Venkatesh, V., Morris, M. G. and Davis, B. G. (2003). User Acceptance of Information Technology : Toward A Unified View. *MIS Quarterly , 27 (3)*, 425-478.
43. Wadlow, T. and Gorelik, V. (2009). Security in the Browser. *ACM Queue , 7(2)*, 40-41.
44. Wang, Xiaoqing and Butler, Brian, "Individual Technology Acceptance Under Conditions of Change" (2003). *ICIS 2003 Proceedings.* Paper 60. http://aisel.aisnet.org/icis2003/60.
45. Whitley, B. E. and others. (1997). Gender differences in computer-related attitudes and behavior: A meta-analysis. *Computers in Human Behavior*, *13*(1), 1–22.
46. Whitside, S.P. and Lynam D.R. (2001). The Five Factor Model and Impulsivity: using structural model of personality to understand impulsivity, *30*, 669-689.
47. Witte, K. (1992). Putting the Fear Back into Fear Appeals: The Extended Parallel Process Model. *Communication Monographs*, 59, 329-349.
48. Wood, W. (2000). Attitude Change : Persuasion and Social Influence. *Annual Review of Psychology, (51)*, 539-570.
49. Woon, I., Tan, G. W., & Low, R. (2005). A protection motivation theory approach to home wireless security. *Proceedings of the Twenty-Sixth International Conference on Information Systems, Las Vegas* (pp. 367–380).