ICBBR Working Paper Series No 2010_07

Brand, Knowledge and False Sense of Security

Wendy Hui

Abstract

A 2x2 experiment was used to study the effects of brand name and knowledge on the adoption of antivirus software. Subjects were randomly assigned to groups and presented with different brands and product choice sets.

It was found that (1) brand name affects product choice, (2) a strong brand may tend to induce a false sense of security and lead to poor product choice, and (3) knowledge can reduce consumers' reliance on brand name in security technology adoption decision.

Keywords

Brand, Knowledge, Experiment, Consumer Market, Technology Adoption

Authors' affiliations

Nottingham University Business School Ningbo, China

Address for correspondence

wendy.hui@nottingham.edu.cn Tel: +8657488180197

Brand, Knowledge and False Sense of Security

Wendy Hui

University of Nottingham Ningbo China, wendy.hui@nottingham.edu.cn

Abstract

A 2x2 experiment was used to study the effects of brand name and knowledge on the adoption of antivirus software. Subjects were randomly assigned to groups and presented with different brands and product choice sets. It was found that (1) brand name affects product choice, (2) a strong brand may tend to induce a false sense of security and lead to poor product choice, and (3) knowledge can reduce consumers' reliance on brand name in security technology adoption decision.

Keywords: Brand, Knowledge, Experiment, Consumer Market, Technology Adoption

1. INTRODUCTION

Consumer security technologies represent a lucrative business, with an expected worldwide market totaling \$3.6 billion USD in 2009 (Gartner Group, 2009). The rapid growth in the consumer segment is partly driven by improved public awareness of information security and an increasing number of Internet-based attacks targeting home users (AusCERT, 2009). Although business opportunities abound in the consumer security technology market, there has not been much investigation in the factors that affect consumers' adoption of security technologies.

Security technologies are different from other information technologies because it is difficult to assess their quality. Information security is defensive in nature and its purpose is to ensure that different parts of an information system do not fail. When this objective is achieved, the achievement is often not observable. Under high quality uncertainty, consumers may rely on product cues such as price (Leavitt, 1954; Tull, Boring, and Gonsior, 1964; McConnell, 1968) and brand (Aaker, 1991) to infer quality. Although brand strength is often positively related to price, in the IT industry, the open source movement has made high quality software available to the public at a very low cost. Thus, the price-quality association may not be as strong as that observed in traditional industries. In this paper, we focus on consumers' use of brand name as a signal for quality.

Our empirical investigation makes use of a 2x2 experimental design to study the interplay between brand, knowledge and perception of security in the context of antivirus software adoption. Our results show that a strong brand tends to induce a greater sense of security and this relationship can be moderated by knowledge. We also discuss the important business implications of our findings.

The rest of the paper is organized as follows. Section 2 reviews the relevant literature and develops the hypotheses. Section 3 describes the research methodology. Section 4 presents the data analysis. Section 5 discusses the business implications of our findings, summarizes the paper, and identifies a number of future research directions.

2. RELEVANT LITERATURE

Early technology adoption research suggests that perceived ease of use, perceived usefulness, computer self-efficacy, perceived behavioral control, and subjective social norm are significant predictors of individual adoption decisions (Davis, 1989; Davis *et al.*, 1989; Compeau and Higgins, 1995; Mathieson, 1991; Taylor and Todd 1995; Harrison *et al.*, 1997). Driven by growing concerns over information security, recent behavioral models of technology adoption begin to take into account risk-related factors including trust and perceived risk (Pavlou and Fygenson, 2006; Pavlou, 2003; Tan and Thoen, 2000). However, few of these studies have examined the role of brand name in consumers' adoption decisions. In this section, we discuss the consumers' tendency to use brand name as a signal of quality of security technologies and how knowledge can reduce this tendency.

Consumers often find it hard to evaluate a security technology due to lack of advanced technical knowledge. According the marketing literature, lack of consumer expertise may force consumers to infer quality based on product cues such as brand (Aaker, 1991). Therefore, a security technology belonging to a strong brand may be perceived to be capable of providing better protection than a weaker brand does. Furthermore, it is possible that the technology's actual quality is lower than its perceived quality. An overestimation of the protection provided can lead to poor product choice. For example, a company sells two antivirus software versions. The basic version provides only malware protection, while the full version provides both malware protection and identity protection that prevents identity theft. A careless computer user who is not aware of common tricks that hackers use to steal passwords and credit card numbers should adopt the full version to prevent identity theft. However, if the company has a strong brand, the user may believe that the lower version is sufficient and buy the basic version instead.

Knowledge about information security threats can reduce consumers' tendency to rely on brand name in their decisions. Spence and Brucks (1997) empirically show that in general, compared to a novice, an expert tends to select fewer but more diagnostic information inputs for consideration and make more

accurate and consistent decisions. Rao and Monroe (1998) show that, as knowledge increases, there is a greater tendency for decision makers to rely more on intrinsic product attributes for product assessments. In a similar vein, Dawar and Parker (1994) report that people who possess more knowledge of personal computers are less likely to use product cues such as brand name when evaluating consumer electronics. Taken together, prior marketing research seems to suggest that, compared to novices, knowledgeable consumers are better at identifying relevant consideration factors, less reliant on brand name and other product cues in their decision-making, and more likely to make good decisions.

3. RESEARCH METHODOLOGY

In this section, we describe a study designed to empirical support three of our hypotheses: (1) brand name affects the adoption decision of a security technology, (2) a strong brand is more likely to lead to a false sense of security, and (3) consumer knowledge can reduce the reliance on brand name in adoption decisions.

3.1 Research Design

We conducted an online survey to test our hypotheses. Our subjects were students in a major English-speaking tertiary institution in China. We decided to study the adoption of antivirus software because it is one of the most commonly used security technologies in the consumer market. Hence, the provision of a detailed explanation about the technology would not be necessary as our subjects should all be familiar with it. We manipulated two factors in our design: the choice set and the brand. This gives us a 2x2 research design as shown in Figure 1.

Choice Set	<u>Group A1:</u> High version: malware and identity protection Low version: malware protection only	<u>Group B1:</u> High version: malware and identity protection Low version: malware protection only
	<u>Group A2:</u> High version: malware and identity protection Low version: identity protection only	<u>Group B2:</u> High version: malware and identity protection Low version: identity protection only
Brand A (Strong Brand)		Brand B (Weaker Brand)
Brand		

Figure 1. Research Design

Two groups of students were assigned to a brand (hereafter “Brand A”) that has the biggest share of the antivirus software industry (61.0% in 2007), while the other two were assigned to a brand (hereafter “Brand B”) with a substantially smaller market share (less than 4.3% in 2007) (CRN, 2007). For each brand, one of the two groups was given the choice between (i) a basic version with malware protection priced at \$40 and (ii) a full version with both malware and identity protection priced at \$60. This type of versioning is common in antivirus software and the version prices are roughly the same as those of similar versions found in the market. The remaining group in each brand was also given a choice between two versions. The basic version was again \$40 and the full version \$60. The full version remained the same. The only difference was that the basic version consisted only of identity protection. Antivirus software that offers only identity protection is less common than software that offers only malware protection. An exception is AVG’s identity protection software.

While the use of an antivirus program with up-to-date virus signatures is generally considered to be essential for PCs, the use of identity protection software is often not listed in identity theft prevention guidelines (e.g., HSBC-North America Military Financial Education Center). A more common suggestion to prevent identity theft is to take good care of passwords, credit card numbers and personal details. Therefore, we expect that when asked to choose between a basic version with only identity protection and a full version, knowledgeable consumers are unlikely to choose the basic version.

An on-demand comparative study conducted by AV-Comparatives (2009a) in February 2009 showed that Brand A could detect 97% of the malware that appeared between May 2008 and early February 2009, while Brand B could detect 93%. In May 2009, AV-Comparatives (2009b) conducted proactive tests on various antivirus products and found that Brand B achieved a proactive detection rate of 45%, while Brand A achieved a rate of 35%. A comparison by Softonic.com (2009) gave Brand A a rating of 4 (out of 5) and Brand B a rating of 4.5 (out of 5) in 2009. In the same year, TopTenReviews.com (2009) gave Brand B a higher ranking than Brand A, but both brands received an overall rating of 3.5 (out of 4). Overall, it seems that the two brands offer comparable levels of protection to their users.

3.2 Measures

Most of our data were collected from an online survey. Near the beginning of the questionnaire, subjects were asked to imagine that they had just purchased a new PC and had to choose between two versions of antivirus software. The version choices each subject received were dependent on their group assignment, which was done randomly. A brief description of the functionalities of each of the presented versions was provided to ensure that the subjects were aware of the difference between the two versions and the type of threats against which each version was capable to defend.

The last part of the questionnaire measured the subjects' knowledge. We decided not to measure knowledge using perception (by items such as "compared to most users, I am among the most knowledgeable in information security") because a discrepancy may exist between what people think they know and what they actually know (DeNisi and Shaw 1997). Instead, we asked the subjects to complete a test on their knowledge about malware and identity theft. The questions mostly came from Internet sources (Abcfraud.ca, Icompute.info). We reviewed the questions and found them appropriate for our research purpose. Minor changes were made to the questions on malware to include rootkits as a type of malware. The final set of questions used in the study is presented in the Appendix. The test score was used as a measure of a subject's knowledge about identity theft and malware. This approach to measure subjects' objective knowledge is consistent with Brucks (1985), Oncken, *et al.* (2005), Tyc, *et al.* (2006), and Weisman, *et al.* (1989).

Demographic data were obtained from the Faculty Office of the tertiary institution.

3.3 Data Collection

Subjects were students from an English-speaking tertiary institution in China. In the academic year 2008-2009, the institution had approximately 3,600 students. All students were invited to complete an online survey. The invitation was sent on May 25, 2009 at around 5:00 pm, and the survey remained open until 11:59 pm, June 8, 2009. Subjects were assured that data were collected only for research purposes and

data analysis would not be done in a personally identifiable manner. Upon the completion of the survey, subjects received a chance to win a digital camera, a mobile phone, and/or an iPod.

There were 844 attempts to complete the questionnaire; 89 were incomplete. Out of these incomplete records, 35 were matched with a complete record based on the student ID number. Three of the completed records were repeated and were therefore removed from the study. Overall, the data suggest that 806 subjects attempted the study, representing a response rate of approximately 22.4%. After the removal of the repeated and incomplete records, the final dataset consisted of 752 usable records.

4. DATA ANALYSIS

The entire student population consisted of 65.5% females. The average age was 20.4 with a standard deviation of 1.3. Table 1 presents summary statistics for the gender and age distributions of our sample of 752 subjects. The gender and age distributions of for each group do not differ significant from those of the target population. Hence, our sample does not seem to exhibit a problem of self-selection bias.

Table 1. Summary Statistics of Demographic Data

Group	Total in Group	Gender	Age
(A1) Brand A, Malware Protection in Basic Version	182	Female: 66.7% Male: 33.3%	Mean: 20.24 S.D.: 1.08
(A2) Brand A, Identity Protection in Basic Version	194	Female: 68.3% Male: 31.7%	Mean: 20.42 S.D.: 1.15
(B1) Brand B, Malware Protection in Basic Version	189	Female: 70.7% Male: 29.3%	Mean: 20.39 S.D.: 1.15
(B2) Brand B, Identity Protection in Basic Version	187	Female: 66.1% Male: 33.9%	Mean: 20.41 S.D.1.25

Table 2 shows the mean and standard deviation of subjects' information security knowledge. As expected from random assignment, subjects' information security knowledge does not seem to differ much across groups.

Table 2. Descriptive Statistics of Subjects' Information Security Knowledge

Group	Mean	S.D.
(A1) Brand A, Malware Protection in Basic Version	11.01	2.74
(A2) Brand A, Identity Protection in Basic Version	10.92	2.90
(B1) Brand B, Malware Protection in Basic Version	11.20	2.76
(B2) Brand B, Identity Protection in Basic Version	10.81	2.67

4.1 Effects of Brand

First, we look at the groups for which the basic version consists only of malware protection, i.e., Groups A1 and B1. If a strong brand leads to a high perceived level of protection, subjects presented with a strong brand are more likely to choose the low version than those presented with a weaker brand. Table 3 presents the percentage of each version choice for both Brand A and Brand B and the result of a z-test comparing the proportion of subjects preferring one version over the other¹. As hypothesized, subjects presented with the strong brand are on average more likely to choose the basic version than those presented with a weaker brand; however, the difference is not statistically significant.

Table 3. Distribution of Version Choice in Groups A1 and B1

Group	Basic Version (Malware Protection Only)	Full Version (Malware and Identity Protection)
(A1) Brand A, Malware Protection in Basic Version	78 (42.9%)	104 (57.1%)
(B1) Brand B, Malware Protection in Basic Version	76 (40.2%)	113 (59.8%)
z-test (1-tailed)	$z = 0.517, p = 0.303$	

On the other hand, in the groups for which the basic version consists only of identity protection (i.e., Groups A2 and B2), the difference is significant. Table 4 again shows that subjects presented with the strong brand are on average more likely to choose the basic version than those presented with a weaker brand. This time, the difference is statistically significant at the 0.05 level. This finding supports our hypothesis that brand name affects adoption decision of security technologies.

Importantly, for these two groups, it is a poor decision to choose only identity protection because malware protection is considered to be essential for PCs, whereas prevention of identity theft can be achieved by non-technical means, such as adopting good password practices and good management of personal information. Hence, the finding also suggests that a strong brand is more likely to induce a false sense of security, which may lead to poor product choice.

¹ The formula used to calculate the z-test results can be found in LeBlanc (2004, p.171).

Table 4. Distribution of Version Choice in Groups A2 and B2

Group	Basic Version (Identity Protection Only)	Full Version (Malware and Identity Protection)
(A2) Brand A, Identity Protection in Basic Version	70 (36.1%)	124 (63.9%)
(B2) Brand B, Identity Protection in Basic Version	50 (26.7%)	137 (73.3%)
<i>z</i> -test (1-tailed)	$z = 1.963, p = 0.025$	

4.2 Effects of Knowledge

To investigate the role of knowledge in version choice, we perform a logistic regression for the groups in which the basic version consists only of malware protection (i.e., Groups A1 and B1). In the logistic regression, we use version choice as the dependent variable, and brand, knowledge and their interaction as the independent variables. The results are presented in Table 5, which shows that knowledge is not a significant predictor of version choice.

Table 5. Logistic Regression Analysis for Groups A1 and B1

(Dependent Variable: Version Choice)

Independent Variables	B	Wald	df	Sig.
Constant	-0.337	0.293	1	0.589
Brand	1.538	2.926	1	0.087
Knowledge	-0.072	1.677	1	0.195
Brand*Knowledge	0.129	2.710	1	0.100

Note: Brand is a dummy variable that has a value of one if it is Brand A and a value of zero otherwise.

Whereas the use of antivirus software is generally considered to be essential, protection against identity theft can be achieved by non-technical means. When knowledgeable consumers are presented with a choice between only malware protection and full protection, they may consider an array of factors including price, need for identity protection by technical means, and the effects on computer performance after the installation of the software. The final choice reflects the consumer's personal preferences and one cannot judge the quality of the decision simply based on the choice made. Since the version choice does not reflect decision quality, the role of knowledge may not be very significant.

On the other hand, knowledge is shown to be an important factor for groups that are presented with only identity protection in the basic version (i.e., Groups A2 and B2). The logistic regression analysis results for these two groups are presented in Table 6. As shown, the more knowledgeable subjects tend to choose the full version instead of the basic version. Furthermore, the effect of knowledge on version choice is significant at the 0.01 level. This finding provides support for our hypothesis that knowledge can alleviate the problem of over reliance on brand name in the evaluation of security technologies.

Table 6. Logistic Regression Analysis for Groups A2 and B2
(Dependent Variable: Version Choice)

Independent Variables	B	Wald	df	Sig.
Constant	-1.628	7.096	1	0.008
Brand	0.889	0.961	1	0.327
Knowledge	0.165	6.961	1	0.008**
Brand*Knowledge	0.040	0.223	1	0.637

Note: Both Version Choice and Brand are dummy variables. Brand has a value of one if it is Brand A and a value of zero otherwise. Version Choice is has a value of one if it is the full version and a value of zero otherwise.

5. IMPLICATIONS, LIMITATIONS AND FUTURE RESEARCH

5.1 Implications

Consumers often face a high level of uncertainty in the assessment of security technologies. As a result, there is a tendency for consumers, especially less knowledgeable ones, to rely on brand name in their adoption decision. Our study empirically shows that brand affects the adoption decision of security technologies. In some cases, a strong brand may induce a false sense of security, resulting in poor product choice. Knowledge about information security can reduce the reliance on the use of brand name in decision-making.

A strong brand is no doubt a valuable asset to a company. However, consumers who overestimate security technologies of a strong brand may end up choosing a product that does not meet their true security needs. If there are different security technologies in a company's product line, poor consumer decisions may lead to undesirable cannibalization effects. Therefore, companies with a strong brand may wish to consider educating consumers and helping them make realistic assessments of the security technologies in their product line. Although this paper focuses on consumer security technologies, our findings can be extended to the organizational context. By offering security education, training and awareness (SETA)

programs, organizations can increase employees' information security knowledge, help them understand the limitations of security technologies, and encourage them to adopt secure computing practices.

5.2 Limitations

We discuss here a limitation in our research design. At the time of writing, a basic version with only malware protection costs 39.99 USD for Brand A and 34.99 USD for Brand B. An advanced version with malware and identity protection costs 69.99 for Brand A (license for 3 PCs) and 54.99 for Brand B. Although the two brands in reality employ different pricing strategies, our research design control for prices and we hope that it has allowed the subjects to focus on perceived quality or protection in their decision-making. It is possible that some subjects are aware of the real pricing strategies of the two brands and this awareness may have an impact on their decisions. We are not sure about the nature of the impact, but it is a potential confounding factor. This limitation is difficult to address because, to study brand effects, one needs a variation in brand strength and since it takes a lot of time and effort to build a strong brand, we believe that creating a strong fictitious brand is not feasible. The downside of relying on real brands is the possibility of introducing confounding factors arising from the idiosyncrasies associated with individual brands investigated, e.g., price.

5.3 Future research

In the future, we wish to replicate our study in different countries to ensure that our findings can be generalized to other cultures. We will continue to explore factors that affect perceived risk, perceived security and security technology adoption. We will also employ an analytical approach to study brand effects on product line management.

APPENDIX

Knowledge on Identity Theft (True or False) (Abcfraud.ca)

1. You need a loan and your credit record is not very good. You go on the internet to see what you can find. Through your research, you find a company that has no complaints or negative feedback. You contact these friendly people and they agree to approve your loan after you have “secured” it with a small fee. This is a no-risk proposition.
2. It is safe to do business over the internet if the website you are looking at looks professional.
3. Promptly respond to any emails you receive, especially if your bank urgently needs your help to fix your account and asks you to confirm your identity.
4. You have the latest computer with a current operating system, virus/spyware detection tools, and a firewall; and you check for and download updates on a daily basis. However, computers cannot be

100% safe. For this reason, you should still be careful when you use your personal information online.

5. You have read and understood everything there is to read about online scams and you now have become a fraud expert in your own right. You can stop worrying about online scams because you are protected and aware.
6. You think you are a victim of identity theft. The first thing you should do is to call your financial institutions and local police.
7. When you get rid of any documents with personal information, such as bank or credit card statements, transaction records, insurance forms or even when you discard your computer hard drive, you should throw them directly in the garbage or recycling bin.
8. When you get your bank account and credit card statements, you should read them and verify that the transactions listed are in fact ones that you made.
9. When you create an email password, you should use your date of birth or that of your spouse or children.
10. The best place to keep your personal identification documents (e.g., passport, birth certificate, citizenship papers) is in your wallet.

Knowledge on Identity Theft (Multiple Choice) (Icompute.info)

(Choices are: a. Trojan, b. Worm, c. Virus, d. Spyware/Adware, e. Rootkit)

1. Which of the listed malware on the right is most likely to make your computer stop working?
2. Which of the listed malware on the right is not a stand-alone program and needs a host to spread itself?
3. Which of the listed malware on the right can spread over the network with little user intervention?
4. Which of the listed malware on the right is less likely to be detected with standard antivirus software?
5. Which of the listed malware on the right is most likely to come with free games, free screensavers, free applications, etc.?
6. Which of the listed malware on the right is bundled with the peer-to-peer file-sharing software, Kazaa?
7. Which of the listed malware on the right is most likely to turn your computer into a “zombie”?
8. Which of the listed malware on the right is most likely to be involved in a distributed denial-of-service attack?
9. Which of the listed malware on the right is the only malware publicly documented as having been employed by the FBI to bring a suspect to trial?
10. Which of the listed malware on the right is most likely to be used for advertising purposes?

REFERENCES

1. Aaker, D. A. (1991), *Managing Brand Equity*. The Free Press, New York.
2. Abcfraud.ca, "Test yourself on online scams," available at: <http://www.abcfraud.ca> (accessed 13 August 2009).
3. AusCERT (2009), "Home users computer security survey 2008," available at: <https://www.auscert.org.au> (accessed 12 August 2009).
4. AV-Comparative (2009a), "On-demand detection of malicious software, anti-virus comparative no. 21, February 2009," available at: <http://www.av-comparatives.org/comparativesreviews> (accessed 12 November 2009).
5. AV-Comparative (2009b), "Proactive/retrospective test (on-demand detection of virus/malware), May 2009," available at: <http://www.av-comparatives.org/comparativesreviews> (accessed 12 November 2009).
6. Brucks, M. (1985), "The effects of product class knowledge on information search behavior," *Journal of Consumer Research*, Vol. 12, June 1985, pp. 1-16.
7. Compeau, D. R. and Higgins, C. A. (1995), "Computer self-efficacy: Development of a measure and initial test," *MIS Quarterly*, Vol. 19, No. 2, pp. 189-211.
8. CRN (2007), "Channel best-sellers: Winning security players," *CRN Magazine*, available at: <http://www.crn.com/security/204200883> (accessed 3 November 2009).
9. Davis, F. D. (1989), "Perceived usefulness, perceived ease of use, and user acceptance of information technology," *MIS Quarterly*, Vol. 13, No. 3, pp. 319-339.
10. Davis, F. D., Bagozzi, R. P. and Warshaw, P. R. (1989), "User acceptance of computer technology: A comparison of two theoretical models," *Management Science*, Vol. 35, No. 8, pp. 982-1002.
11. Dawar, N. and Parker, P. (1994), "Marketing universals: Consumers' use of brand name, price, physical appearance, and retailer reputation as signals of product quality," *The Journal of Marketing*, Vol. 58, No. 2, pp. 81-95.
12. DeNisi, A. S. and Shaw, J. B. (1977), "Investigation of uses of self-reports of abilities," *Journal of Applied Psychology*, Vol. 63, pp. 641-644.
13. Gartner Group (2009), "Gartner says worldwide security software market on pace to grow 8 per cent in 2009," available at: <http://www.gartner.com> (accessed 23 November 2009).
14. Harrison, D. A., Mykytyn, P. P. and Riemenschneider, C. K. (1997) "Executive decisions about adoption of information technology in small business: Theory and empirical tests," *Information Systems Research*, Vol. 8, Vol. 2, pp. 171-195.

15. HSBC-North America Military Financial Education Center, University of Maryland University College, "How to prevent identity theft," available at: <http://militaryfinance.umuc.edu> (accessed 12 November 2009).
16. Icompute.info, "Malware quiz," available at: <http://www.icompute.info> (accessed 13 August 2009).
17. LeBlanc, D. C. (2004), *Statistics: Concepts and Applications for Science*, Jones & Bartlett Publishers.
18. Leavitt, H. J. (1954), "A note on some experimental findings about the meaning of price," *Journal of Business*, Vol. 27, 205-210.
19. Mathieson, K. (1991) "Predicting user intentions: Comparing the technology acceptance with the theory of planned behavior," *Information Systems Research*, Vol. 2, No. 3, pp. 173-191.
20. McConnell, J. D. (1968), "An experimental examination of the price-quality relationship," *Journal of Business*, Vol. 41, pp. 439-444.
21. Oncken, C., McKee, S., Krishnan-Sarin, S., O'Malley, S. and Mazure, C. M. (2005), "Knowledge and perceived risk of smoking-related conditions: A survey of cigarette smokers," *Preventive Medicine*, Vol. 40, No. 6, pp. 779-784.
22. Pavlou, P. A. and Fygenson, M. (2006), "Understanding and predicting electronic commerce adoption: An extension of the theory of planned behavior," *MIS Quarterly*, Vol. 30, No. 1, pp. 115-143.
23. Pavlou, P.A. (2003), "Consumer acceptance of electronic commerce: integrating trust and risk with the Technology Acceptance Model," *International Journal of Electronic Commerce*, Vol. 7, No. 3, pp. 69-103.
24. Rao, A. R. and Monroe, K. B. (1988), "The moderating effect of prior knowledge on cue utilization in product evaluations," *Journal of Consumer Research*, Vol. 15, September, 1988, pp. 253- 264.
25. Softonic.com (2009), "Comparison of Norton antivirus with other programs, 2009," available at: <http://norton-antivirus.en.softonic.com> (accessed 12 November 2009).
26. Spence, M. T. and Brucks, M. (1997), "The moderating effects of problem characteristics on experts' and novices' judgments," *Journal of Marketing Research*, Vol. 34, No. 2, pp. 233-247.
27. Tan, Y. H., and Thoen, W. (2000), "Toward a generic model of trust for electronic commerce," *International Journal of Electronic Commerce*, Vol. 5, Vol. 2, pp. 61-74.
28. Taylor, S. and Todd, P. A. (1995), "Understanding information technology usage: A test of competing models," *Information Systems Research*, Vol. 6, No. 4, pp. 167-176.
29. TopTenReview.com (2009), "AntiVirus Software Review Product Comparisons," available at: <http://anti-virus-software-review.toptenreviews.com> (accessed 12 November 2009).
30. Tull, D. S., Boring, R. A. and Gonsior, M. H. (1964), "A note on the relationship of price and imputed quality," *Journal of Business*, Vol. 38, April, 1964, pp. 186-191.

31. Tyc, V. L., Lensing, S., Rai, S. N., Klosky, J. L., Stewart, D. B. and Gattuso, J. (2006), "Predicting perceived vulnerability to tobacco-related health risks and future intentions to use tobacco among pediatric cancer survivors," *Patient Education and Counseling*, Vol. 62, No. 2, pp. 198-204.
32. Weisman, C. S., Nathanson, C. A., Ensminger, M., Teitelbaum, M. A., Robinson, J. C. and Plichta, S. (1989), "AIDS knowledge, perceived risk and prevention among adolescent clients of a family planning clinic," *Family Planning Perspectives*, Vol. 21, No. 5, pp. 213-217.
33. Whitman, M.E. and Mattord, H. J. (2007), *Principles of Information Security*, 3rd Edition, Course Technology.