Uncertainties of Online Phishing Risks and Consumer Decision Making in B2C E-Commerce

Ping An Wang, *Member, IAENG*

***Abstract* – Phishing has been a growing information security risk for online consumers. However, various levels of uncertainties exist in consumer knowledge and evaluation of online phishing risks. Drawing upon research in decision under risks and uncertainties, this study categorizes an online consumer's knowledge of phishing risks as falling under one of four uncertainty states: known certainty, known uncertainty, unknown uncertainty, and unknowable uncertainty. This research focuses on the effect of uncertainty levels of e-commerce consumers' knowledge of phishing risks on their online purchase intentions and decision. A series of four group experiments were conducted with the four uncertainty states as treatments among 120 subjects. The experimental results indicate that consumer willingness to pay and intention to purchase vary systematically under different uncertainty levels of knowledge of phishing risks.**

***Index Terms* – E-commerce, intention to purchase, phishing, uncertainties, willingness to pay**

I. INTRODUCTION

Phishing has been a serious online risk related to privacy, security, and trust and is still a phenomenon of great practical significance for B2C (business-to-consumer) e-commerce [3]. Phishers often try to lure victims into clicking a spoofed universal resource locator (URL) pointing to a rogue Web page to steal sensitive personal and financial information from unsuspecting online consumers [11]. There has been considerable research on online risks and consumer decision making in the B2C e-commerce context [2, 19, 26]. However, existing research primarily focuses on determinants of subjective probability and value and assumes that consumers judge i) the subjective probability of a loss, and, ii) the subjective magnitude of consequences of the loss, and compute an expectation of loss. A significant problem is that neither the probability of occurrence of online risks nor the consequences of risky events are always known to consumers. For example, the likelihood and consequences of a credit card fraud resulting from an online transaction are not known for sure even to experts [17]. Thus, the question arises as to how online consumers judge phishing risks and decide on online purchases under various uncertain knowledge conditions of the risks.

This study argues that consumer decisions in risky online environments are made under uncertain conditions where risk probability information is imprecise, vague, or ambiguous. Based on research in decision under risks and uncertainties, this study categorizes an online consumer's knowledge of the phishing risk as falling under one of four fine-grained uncertainty states: known certainty, known uncertainty, unknown uncertainty, and unknowable uncertainty. An online consumer's risk evaluation and purchase intention and decision are strongly affected by his or her assumption of the variant of uncertainty regarding the extent and severity of the phishing security risk involved in the online transaction.

The primary goal of this research is to investigate how variant degrees of uncertainty of online consumers' knowledge of phishing risks affect their judgment of and behavioral response to the risks. Section II below reviews relevant information systems (IS) literature on decision under risks and uncertainty. Section III discusses the research model and hypotheses proposed. Section IV introduces the experiment method used for the study. Section V reports the data analysis and findings. Section VI concludes the paper.

Manuscript draft was received on January 2, 2011; revised and resubmitted on January 30, 2011.

Ping An Wang, PhD, is Professor of Computer Information Technology at Allegheny County College South Campus in Pittsburgh, PA, USA 15122 (Contact phone: 412-469-6320; email: pwang@ccac.edu).

ISBN: 978-988-18210-6-5
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

II. LITERATURE REVIEW

There has been considerable IS research interest in decision under uncertainty and the impacts of online security risks. However, there has not been a systematic model and approach available to address the impacts of variant uncertainties of knowledge of online information security risks on consumer decision making in the B2C e-commerce context. The theoretical basis for prior research on decision under risk and uncertainty primarily falls into three categories: utility theory, attitudinal theories, and the psychometric paradigm.

A. Risk Studies Based on Utility Theory

The classical notion of risk in decision theory is primarily modeled using utility theory. Utility theory assumes that people are rational and should choose the option that maximizes the expected utility, which is the product of probability and payoff. Utility theory also assumes that all risk probabilities and payoff are known to a point estimate but does not allow ambiguity, or a variant form of uncertainty. In reality, however, uncertainty does occur when risk probabilities or payoff is missing or unknown. The subjective expected utility (SEU) model of utility theory proposed by Savage [22] argues that people's *subjective* preferences and beliefs, rather than objective probabilities, are used in the evaluation of an uncertain prospect for decision making. The SEU model is based on a set of seven axioms designed for consistent and rational behavior.

Subsequent research, however, has shown that people often violate the axioms [23]. Experimental studies by Ellsberg [6] indicated that the choices of many decision makers reveal inconsistent preferences that cannot be explained using the SEU model. Ellsberg's experiment demonstrated that people prefer known and specific probabilities to ambiguity or vagueness, suggesting ambiguity aversion. But Ellsberg did not address the factor of unknowable uncertainty in decision making. In addition, Ellesberg's experimental study was limited to urn tasks and choices for bets.

Another variation of utility theory is the prospect theory proposed by Kahneman and Tversky [14]. The prospect theory views decision under risks from a behavioral economic perspective and recognizes the importance of framing perceptions in risk and outcome evaluation. Kahneman and Tversky argued that attitudes toward risk are jointly determined by perceived values and decision weights of specified prospects or choices. The prospect theory presented a descriptive conceptual model for framing risk perceptions, but it does not address security risks in e-commerce. Also, it is usually a difficult task to determine and measure the reference point for gains and losses. In reality, very few IS research articles use this theory [17].

The maxmin expected utility (MEU) model proposed by Gilboa and Schmeidler [12] argues that a decision maker has a set of prior beliefs and the utility of an act is the minimal expected utility in this set. However, the model did not differentiate uncertainty levels and failed to address the role of subjective beliefs in decision making under uncertainty. The comparative ignorance hypothesis by Fox and Tversky [9] argued that ambiguity aversion is produced by a comparison with less ambiguous events or with more knowledgeable individuals. Like other utility theory approaches, their study neither distinguished different degrees of uncertainty nor studied online phishing risks.

B. Risk Studies Based on Attitudinal Theories

A large amount of prior research on online risks was based on attitudinal theories involving risk perceptions and behavioral intentions. The conceptual assumption of such models was rooted in the theory of reasoned action (TRA) developed by Fishbein and Ajzen [8]. In TRA, behavioral intentions, determined by attitudes and perceptions, are antecedents to specific individual behaviors. An online customer's perception and attitudes regarding risks, accordingly, will affect his or her behavioral intentions to conduct transactions online. The general assumption of various attitudinal theories is that people's decisions under risks are driven by inconsistent perceptions, beliefs, and emotions.

Hogarth and Kunreuther [13] found uncertainty of risk knowledge an important factor in consumer decision making. The study was one of the few applied to consumer purchase decisions, but it did not involve online security risks. However, they pointed out that the standard lab cases of gambling used in most prior decision studies did not capture the variety of decision choices faced by people in the real world. Roca, Hogarth, and Maule [28] concurred that future decision research should be extended to a broader range of contexts and response modes, such as willingness to pay for uncertainties and risks.

Bhatnagar et al. [2] suggested a negative correlation between knowledge and risk aversion. However, their study focus was not on online security risks but on product risks and financial risks. Miyazaki and Fernandez [16] studied the relationship between consumer perceived privacy and security risks and online purchase behavior. Salisbury et al. [21] studied consumer perceptions of Web security risks in Internet shopping. Pavlou [18] proposed a B2C e-commerce acceptance model of trust, perceived risk, perceived usefulness, and ease of use for predicting e-commerce acceptance and online purchase behavior. Milne et al. [15] studied the online privacy risks from the security perspective and focused on the specific risk of identity theft. However, none of these studies included the consumer risk knowledge factor or uncertainty levels in addressing consumer purchase decisions.

Aquisti and Grossklags [1] recognized the importance of uncertainty in individual decision making in situations that have an impact on privacy. Their concept of privacy risks is relevant to the domain of online information security. However, they did not address the security knowledge factor in e-commerce decision making. Tsai et al. [27] studied the role of privacy policy visibility and privacy protection concerns in online shopping decisions. They found that online consumers value privacy and are willing

ISBN: 978-988-18210-6-5
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

to pay a premium for privacy protection. However, they did not address knowledge or uncertainty factors for individual decision making.

The common assumption of the prior studies from various attitudinal perspectives is that decisions under risks are driven by inconsistent perceptions, beliefs, and emotions. However, they all share two major limitations: a) no presence of fine-grained degrees of uncertainties, and b) lack of focus on the online phishing risks and e-commerce consumer decision making.

C. The Psychometric Approach to Risks

Prior IS research based on the psychometric theory suggests that consumers use attributes other than risk probabilities and consequences in their decision making. Fischhoff et al [7] studied technological risks and benefits using the psychometric paradigm. The study touched upon known and unknown risks but did not address the unknowable risks. Slovic et al. [25] found that risk acceptability is affected by risk attributes, such as familiarity, control, and uncertainty about the level of risk. However, they neither defined the uncertainty concept nor distinguished different degrees of uncertainty of risk knowledge. Slovic [24] further suggested that the level of knowledge attribute seems to influence the relationship between perceived risk, perceived benefit, and risk acceptance. However, he did not distinguish different degrees of uncertainties. Also, his study did not touch upon any online security or phishing risks for e-commerce.

Nyshadham and Ugbaja [17] used psychometric techniques to study how B2C e-commerce consumers organize novel online risks in memory. The study called for further analysis to define the risk dimensions. Using the psychometric paradigm, Gabriel and Nyshadham [10] studied perceptions of online risks that affect online purchase intentions in the B2C e-commerce environment. The focus of the study was to develop a taxonomy of online risks and construct a cognitive map of online consumers' risk perceptions and attitudes. The results suggested that knowledge of risks is an important parameter of online risk perceptions. However, the study did not focus on the variable of knowledge and did not go into fine-grained notion of risk probability.

This research is to address the common limitations of prior studies by focusing on the uncertainty of knowledge of online phishing risks in e-commerce decision making and adopting a fine-grained taxonomy of degrees of uncertainties. The purpose of the study is to measure the effect of knowability of risk on a person's decision making when faced with online phishing risks. Chow and Sarin [4] defined knowability as one's assumption about the availability of information regarding the uncertainty of probability. Decision situations are usually either under certainty or uncertainty. In contrast to known certainty, Chow and Sarin proposed and distinguished three types of uncertainties: known, unknown, and unknowable uncertainties. This fine-grained classification of uncertainties of risk knowledge is the theoretical basis for this study. Accordingly, the uncertainties are broken down into four levels or degrees of conditions: known certainty, known uncertainty, unknowable uncertainty, and unknown uncertainty. Table I below defines the four degrees of uncertainties with examples.

Table I. Uncertainties of Risk Knowledge

Degree of Uncertainty	Definition	Example
Known Certainty	Information on all attributes and alternatives are available.	A vendor guarantees that none of its online transactions involves phishing, due to strong online security mechanism.
Known Uncertainty	Risk probability is precisely and officially specified.	It is officially confirmed that 3% of online transactions with the vendor involve phishing.
Unknowable Uncertainty	Risk probability is unavailable to all.	It is impossible for anyone to know exactly what percentage of online transactions with the vendor involves phishing.
Unknown Uncertainty	Risk probability is missing to one but may be possessed by others.	The public is only told that less than 5% online transactions with the vendor involve phishing. But the exact percentage is not disclosed.

III. RESEARCH MODEL

The research model, shown in Fig. 1 below, is used to guide this study.

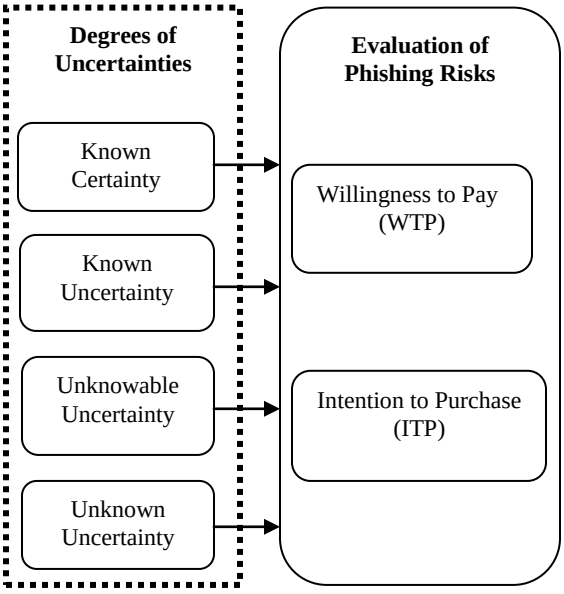

Fig. 1. Research Model. Adapted from Wang [28].

ISBN: 978-988-18210-6-5
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

The research model is contextualized for the different degrees of uncertainties of risk knowledge. The construct of phishing risk evaluation reflects consumers' subjective beliefs and judgment of online phishing risks and protection mechanisms. Decision behaviors under risks are related to people's degrees of knowledge of the risk probabilities. Hogarth and Kunreuther [13] found that people demonstrate different observable behaviors between situations where they do and do not have knowledge about probabilities and outcomes. Thus, uncertainty levels of risk knowledge affect decision under risks.

Known certainty is obviously the ideal knowledge level for decision making. The constructs of variant uncertainties are based on Chow and Sarin [4]. Chow and Sarin view known uncertainty as the most comfortable uncertainty to people and preferable to vagueness in probability. Unknown uncertainty is less preferable than unknowable uncertainty, and it is the least comfortable level of uncertainty to a decision maker. Unknowable uncertainty, according to Chow and Sarin, is the intermediate comfort level of uncertainty to people and more tolerable than unknown uncertainty. Thus, the following two hypotheses are proposed for this study:

Hypothesis 1: Known uncertainty is preferable to unknowable uncertainty in consumer evaluation of online phishing risks.

Hypothesis 2: Unknowable uncertainty is preferable to unknown uncertainty in consumer evaluation of online phishing risks.

Consumers' behavioral response to risks consists of willingness to pay (WTP) to avoid the risk and intention to purchase (ITP) online. Prior research in decision theories suggested that individuals are willing to pay a premium to avoid uncertainty of risks [4, 20]. The WTP amount is expected to grow as consumer perceived phishing risk increases. In addition, according to the theory of reasoned action (TRA), attitudes and perceptions determine behavioral intentions which are antecedents to actual behavior. Thus, ITP is expected to decrease as the perceived phishing risk level increases.

IV. METHODOLOGY

An experiment was used to test the research model. Variant degree of uncertainty is the key treatment variable, and WTP and ITP are the primary dependent variables. The design of the experiment and questions were based on the experiments developed and pilot tested by Wang [28].

The experiment was conducted among a total of 120 undergraduate students recruited from a college in northeastern United States. The subjects were randomly divided into four groups, each receiving a different uncertainty treatment: known certainty (KC), known uncertainty (KU), unknowable uncertainty (UBU), and unknown uncertainty (UNU). The treatment variable was induced among subjects using hypothetical risk scenarios and vignettes of online phishing adapted from Wang [28]. Each vignette depicts an online phishing risk scenario corresponding to a different uncertainty degree in Table I above. Based on the vignette, subjects provided judgments on the amount they are willing to pay (WTP) to avoid the risk and intention to purchase (ITP) online. An analogy type manipulation check question was also given to check if the treatment variable was properly understood by the subject. In addition, demographic data were collected from subjects at the end of the experiment.

V. DATA ANALYSIS AND RESULTS

A total of 120 responses were received from the four group experiments. A total of three responses were found to have failed the manipulation check question and were excluded from data analysis.

A. Demographics

Basic data on demographics and relevant online experience were collected from the subjects. The data include age, gender, Internet usage, and experience in online purchase and online credit card payment. The data show that over 90% of the subjects have had prior experience purchasing online and making online payment by credit card. In addition, over 80% of the subjects have used the Internet for four or more years. On average, over 95% of the subjects use the Internet between 1 and 10 hours per day. The age of the subjects for the pilot study falls between 18 and 50. The gender ratio of the subjects (56% female and 44%) male is very close to the gender ratio of the general student population at the sampled college.

B. ANOVA Results

ANOVA was performed on WTP and ITP using the uncertainty treatment level as the independent variable. The ANOVA results suggest that the subjective estimates on willingness to pay to avoid the online phishing risk and on the scale of intention to purchase online are significantly different across the four treatment levels in the experiment. This shows that variant uncertainty levels have a significant effect on online consumer decisions.

Follow-up post hoc tests were conducted using SPSS to compare the pairwise differences among the means of WTP and ITP. Tables II and III below display the test output. The results of both tests for indicate significant differences across the treatment conditions for both WTP and ITP. Table II shows that consumers are willing to pay a statistically significant amount of approximately $2.50 to avoid moving from known uncertainty to unknowable uncertainty and approximately $3.50 to avoid moving from unknowable uncertainty to unknown uncertainty in judging online phishing risk scenarios.

In terms of the ITP measure, Table III suggests that online consumers have statistically greater intentions to purchase online under reduced uncertainty conditions. Table III shows that the average intention to purchase under the knowable uncertainty condition is 1.5667 greater than that under the unknowable condition. The average ITP under unknowable uncertainty is 2.4138 greater than that under the unknown uncertainty condition.

ISBN: 978-988-18210-6-5
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

Table II. Tukey Post Hoc Tests for WTP

	(I) Treatment	(J) Treatment	Mean Difference (I-J)
Tukey HSD	KC	KU	-2.4503(*)
		UBU	-4.9466(*)
		UNU	-8.4601(*)
	KU	KC	2.4503(*)
		UBU	-2.4963(*)
		UNU	-6.0098(*)
	UBU	KC	4.9466(*)
		KU	2.4963(*)
		UNU	-3.5135(*)
	UNU	KC	8.4601(*)
		KU	6.0098(*)
		UBU	3.5135(*)

* The mean difference is significant at the .05 level.

Table III. Tukey Post Hoc Tests for ITP

	(I) Treatment	(J) Treatment	Mean Difference (I-J)
Tukey HSD	KC	KU	1.2667(*)
		UBU	2.8333(*)
		UNU	5.2471(*)
	KU	KC	-1.2667(*)
		UBU	1.5667(*)
		UNU	3.9805(*)
	UBU	KC	-2.8333(*)
		KU	-1.5667(*)
		UNU	2.4138(*)
	UNU	KC	-5.2471(*)
		KU	-3.9805(*)
		UBU	-2.4138(*)

* The mean difference is significant at the .05 level.

VI. CONCLUSION

This study proposed a fine-grained approach to understanding variant degrees of uncertainties of consumer knowledge of online phishing risks. The goal of the study was to investigate the effect of variant levels of uncertainties on B2C e-commerce consumer decision making in online purchase. The experimental results provided empirical support for the research model and the hypotheses of this study. The finding suggests that consumer judgment of online phishing risks and intention to purchase vary systematically with the uncertainty conditions of their risk knowledge. The pairwise differences for WTP and ITP indicate that consumers prefer known uncertainty over unknowable uncertainty over unknown uncertainty in this order in judging online phishing risks. This study can be further extended to future studies of other online security risks involving decision under uncertainty.

A practical implication of the finding of this study is for B2C e-commerce vendors. The research suggests that online vendors may increase consumer intention to purchase by lowering uncertainty and presenting online phishing risks with more precise risk probability and outcome estimates.

REFERENCES

[1] Acquisti and J. Grossklags, "Uncertain, Ambiguity, and Privacy," *Proceedings of the 4th Annual Workshop on Economics and Information Security*, 2005, pp. 1-21.
[2] Bhatnagar, S. Misra, and H.R. Rao, "On Risk, Convenience, and Internet Shopping Behavior," *Communications of the ACM*, vol. 43, no. 11, 2000, pp. 98-105.
[3] Bose and A.C.M. Leung, "Unveiling the masks of phishing: Threats, preventive measures, and responsibilities," *Communications of the Association for Information Systems,19*, 2007, pp. 544-566.
[4] C.C. Chow and R.K. Sarin, "Known, Unknown, and Unknowable Uncertainties," *Theory and Decision*, no.52, 2002, pp. 127-138.
[5] T. Dinev and Q. Hu, "The Centrality of Awareness in the Formation of User Behavioral Intention toward Protective Information Technologies," *Journal of the Association for Information Systems*, vol. 8, July 2007, pp. 386-408.
[6] D. Ellsberg, "Risk, Ambiguity and the Savage Axioms," *Quarterly Journal of Economics*, no. 75, 1961, pp. 643-669.
[7] B. Fischhoff, P. Slovic, and S. Lichtenstein, "How Safe is Safe Enough? A Psychometric Study of Attitudes Towards Technological Risks and Benefits," *Policy Sciences*, vol. 9, no. 2, 1978, pp. 127-152.
[8] M. Fishbein and I. Ajzen, *Belief, Attitude, Intention,and Behavior: An Introduction to Theory and Research*, Reading, MA: Addison-Wesley, 1975.
[9] C.R. Fox and A. Tversky, "Ambiguity Aversion and Comparative Ignorance," *The Quarterly Journal of Economics*, vol. 110, no. 3, 1995, pp. 585-603.
[10] I.J. Gabriel and E. Nyshadham, "A Cognitive Map of People's Online Risk Perceptions and Attitudes: An Empirical Study," *Proceedings of the 41st Annual Hawaii International Conference on Systems Sciences*, 2008, Big Island, HI, pp. 274-283.
[11] S. Garera, N. Provos, M. Chew, and A.D. Rubin, "A framework for detection and measurement of phishing attacks," *WORM'07, November 2, 2007, Alexandria, VA*, 1-8.
[12] I. Gilboa and D. Schmeidler, "Maxmin Expected Utility with Non-unique Prior," *Journal of Mathematic Economics*, no. 18, 1989, pp.141-153.
[13] R.M. Hogarth and H. Kunreuther, "Decision Making Under Ignorance: Arguing With Yourself," *The Journal of Risk and Uncertainty*, no. 10, 1995, pp. 15-36.
[14] D. Kahneman and A. Tversky, "Prospect Theory: Analysis of Decision Under Risk," *Econometrica*, vol. 47, no. 2, pp. 263-292.
[15] G.R. Milne, A.J. Rohm, and S. Bahl, "Consumers' Protection of Online Privacy and Identity," *The Journal of Consumer Affairs*, vol. 38, no.2, pp. 217-232.
[16] A.D. Miyazaki and A. Fernandez, "Consumer Perceptions of Privacy and Security Risks for Online Shopping," *The Journal of Consumer Affairs*, vol. 35, no. 1, 2001, pp. 27-44.
[17] E.A. Nyshadham and M. Ugbaja, "A Study of Ecommerce Risk Perceptions among B2C Consumers: A Two Country Study," *Proceedings of the 19th Bled eConference*, Bled, Slovenia, 2006.
[18] P.A. Pavlou, "Consumer Acceptance of Electronic commerce: Integrating Trust and Risk with the Technology Acceptance Model," *International Journal of Electronic Commerce*, vol. 7, no. 3, 2003, pp. 69-103.
[19] P.A. Pavlou and M. Fygenson, "Understanding and Predicting Electronic Commerce Adoption: An Extension of the Theory of Planned Behavior," *MIS Quarterly*, vol. 30, no. 1, 2006, pp. 115-143.
[20] M. Roca, R.M. Hogarth, and A.J. Maule, "Ambiguity Seeking As A Result of the Status Quo Bias," *The Journal of Risk and Uncertainty*, no. 32, 2002, pp. 175-194.

ISBN: 978-988-18210-6-5
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

[21] W.D. Salisbury, R.A. Pearson, A.W. Pearson, and D.W. Miller, "Perceived Security and World Wide Web Purchase Intention," *Industrial Management & Data Systems*, vol. 101, no.4, pp. 165-176.
[22] L.J. Savage, *The Foundations of Statistics*. New York: Wiley, 1954. (Revised and enlarged edition), New York: Dover, 1972.
[23] G. Shafer, "Savage Revisited," *Statistical Science*, vol. 1, no. 4, 1986, pp. 463-501.
[24] P. Slovic, "Perception of Risk," *Science*, no. 236, 1987, pp. 280-285.
[25] P. Slovic, B. Fischhoff, and S. Lichtenstein, "Why Study Risk Perception?" *Risk Analysis*, vol. 2, no. 2, 1982, pp. 83-93.
[26] J. Son and S.S. Kim, "Internet Users' Information Privacy-protective Responses: A Taxonomy and A Nomological Model," *MIS Quarterly*, vol. 32, no. 3, 2008, pp. 503-529.
[27] J. Tsai, L. Cranor, S. Egelman, and A. Acqusiti, "The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study," *Proceedings of the Twenty Eighth International Conference on Information Systems*, Montreal, Canada, pp. 1-17.
[28] P. Wang, "The effect of knowledge of online security risks on consumer decision making in B2C e-commerce," Ph.D. dissertation, Grad. School of Computer &Info. Sciences, Nova Southeastern Univ., Ft. Lauderdale, FL, 2010, (UMI No. 3422425).

ISBN: 978-988-18210-6-5
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)