View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by AIS Electronic Library (AISeL)

Association for Information Systems
AIS Electronic Library (AISeL)

SAIS 2017 Proceedings | Southern (SAIS)

3-25-2017

Consumer Perceptions about E-Commerce- The Influence of Public Internet Trust

Lakshman Mahadevan
Rajagiri Centre for Business Studies, lakshman@rajagiri.edu

Jeffrey P. Kaleta
Georgia Southern University, jeff.kaleta@gmail.com

Follow this and additional works at: http://aisel.aisnet.org/sais2017

Recommended Citation
Mahadevan, Lakshman and Kaleta, Jeffrey P., "Consumer Perceptions about E-Commerce- The Influence of Public Internet Trust" (2017). *SAIS 2017 Proceedings*. 15.
http://aisel.aisnet.org/sais2017/15

This material is brought to you by the Southern (SAIS) at AIS Electronic Library (AISeL). It has been accepted for inclusion in SAIS 2017 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.

CONSUMER PERCEPTIONS ABOUT E-COMMERCE - THE INFLUENCE OF PUBLIC INTERNET TRUST

Lakshman Mahadevan
Rajagiri Centre for Business Studies
lakshman@rajagiri.edu

Jeffrey P. Kaleta
Georgia Southern University
jkaleta@georgiasouthern.edu

ABSTRACT

Access to the internet from public places has further strengthened the internet as an anywhere-everywhere concept. Globally more businesses offer free public Wi-Fi for their customers. This research looks at customer attitude towards the use of free public Wi-Fi for e-commerce transactions, specifically, how does trust of the free public internet influence customer perception of the security of the e-commerce retailer websites. We conduct a brief study of participants in both the US and India on their perceptions of conducting e-commerce transactions using free public Wi-Fi. Our results show that the trust of the free public internet is a significant predictor of perceived security of the e-commerce website. Encrypted connections notwithstanding, businesses may need to stress the message that their website is safe to transact over public Wi-Fi.

Keywords

Public internet, free Wi-Fi, e-commerce, trust, consumer behavior

INTRODUCTION

E-commerce web sites of their own accord offer a great deal of security to their consumers by offering encryption for consumer transactions, as well as securing consumer information such as their address, phone number and credit card numbers (Marchany and Tront, 2002; Salam et al., 2003). Against this backdrop are constant messages from media outlets (e.g. Pullen, 2016; Forbes, 2015) replete with incidents of how public internet has become a conduit to sniff out personal information of consumers. Provided this barrage of disparaging views of public internet, it is important to understand how consumers perceive web site security, specifically their perception of secure encrypted connections as they shop online over free public internet. Previous literature has focused a great deal on perceived security of the website (Hartono et al., 2014; Roca et al., 2009) and consumer attitudes to online shopping (Gefen et al., 2003; Hasan, 2010; Zhou et al., 2007). However, little or no research has looked at perceptions consumers have about the security offered by the website when consumers shop from public spaces using free Wi-Fi. Therefore, our research asks the following question.

How does trust of free public internet impact perceived security of the e-commerce website and consumer attitudes?

PUBLIC INTERNET TRUST

From the perspective of using public internet as a channel to transact with e-commerce websites, consumers need to have a favorable opinion about the ability of the public internet to protect sensitive transaction information such as username, passwords, and credit card numbers. Although information transferred back and forth between the consumer and the e-commerce website is reasonably secure (Chenoweth et al.,2010), public internet is prone to electronic sniffing (Klasnja et al., 2009; Mukherjee and Nath, 2007) made easier by the use of open un-encrypted Wi-Fi networks (Ferreira et al., 2011). Also, public internet needs to ensure adequate speedy response and no loss of connection to bolster consumer's perceptions of security and reliability. It would not augur well for the consumer and nor for the e-commerce website if the connection responds quickly to one request but takes inordinate time with another. Should consumers lose connection to a retailer website after submitting credit card information, there is no confirmation for the consumer to ensure if the e-commerce website received the information and the order was indeed placed. The reliability as well as the safety offered by the internet connection is an important factor in conducting e-commerce transactions and thus becomes an object of consumer trust (Corritore et al., 2003; Pennington et al., 2003-2004; Ratnasingam, 1998; Rotchanakitumnuai and Speece, 2003; Shankar et al., 2002). We define public internet trust on Grabner-Krauter and Faullant (2008) conceptualization of internet trust as the trusting beliefs in the reliability and predictability of the internet and the willingness of the consumer to depend on the internet with regard to economic transactions.

PERCEIVED WEBSITE SECURITY

E-commerce websites offer a host of security measures to ensure customers have a safe and secure transaction. Security measures are of two types. First is to ensure customers have a secure environment at the time of transacting with the e-commerce site. For instance, encrypted channels and security messages are some of the measures websites provide that ensure a secure transactional environment (Chellappa and Pavlou, 2002; LaRose and Rifon, 2007). Second, to ensure e-commerce websites store customer information, such as shopping preferences, username/password, previous purchases, and credit card information, is secure and out of harm's way (Gefen et al., 2003). Therefore, we define perceived website security (PWS) as the mitigation of a threat facing an e-commerce website that creates a circumstance, condition, or event with the potential to cause economic hardship to data or network resources in the form of destruction, disclosures, and modification of data, denial of service, and/or fraud, waste and abuse (Kalakota and Whinston, 1997, p. 853).

HYPOTHESES DEVELOPMENT

Consumers use the public internet for various activities such as searching for news, watching online videos, weather conditions, communicating with friends over WhatsApp and Facebook. Jarvenpaa et al. (2000) report that consumers develop online trust through positive interactions with the e-commerce website. Repeated successful consummation of such interactions improves perceptions about the public internet as a reliable and trusted channel. However, when consumers use the free public internet to transact with an e-commerce website, personal information passes back and forth between the e-commerce website and the consumer. Website security partly relies on transmission of secure information between the consumer and the website. Liu et al. (2005) state that a primary reason why many people have yet to adopt online shopping is due to the lack of trust between the customer and the online site. This lack of trust inhibits consumers in providing personal or credit card information, despite huge investment in security technology such as privacy seal programs, authentication mechanisms and encryption (Mukherjee and Nath,2007; Riquelme and Roman, 2014).

However, Hartono et al. (2014) report the need for websites to maintain confidentiality of consumer information, ensuring that transactional information is preserved and recorded correctly. The trust deficiency could be due to the lack of understanding of what role the internet channel plays in the perception about e-commerce website security. Byrd (2011) states that the local infrastructure is a key vulnerability point in an online transaction. Un-trusted infrastructure or networks contain vulnerabilities that provide hackers with targets to compromise victim's information (Lee et al., 2016). It is possible that with increased confidence about the capability of the public internet to transmit information securely, consumer's perception of the e-commerce website security also improves. For instance, the public internet connection could fail in the midst of a transaction, creating insecurity in the mind of the customer who is thinking about all the personal information just provided. Here questions about the website security arise for not having responded in a timely fashion to the customer request. Yet another instance, where a hacker sniffs customer information out, it results in unauthorized purchases using the customer's account. Here again, the consumer questions website security whereas the culprit is the public internet. When there is confidence about the transmission and reception of secure information, there is an improved perception about the security provided by e-commerce website. Thus, we propose that:

> H1: Increased trust of the public internet leads to increased perceived security of the e-commerce website.

Customers rely on electronic payment methods to transact with an e-commerce website over the public internet. In general, consumers are usually comfortable providing general information such as preferences, but not as comfortable to provide sensitive information such as credit card numbers and account information (Palvia, 2009). People's perception of the security of websites is an important factor for online purchase decisions (Chang and Chen, 2009). With increased perceived security, consumers have more confidence in sharing their credit card numbers and other personal details with the e-commerce website and ready to consummate the exchange (Salisbury et al., 2001; Cheng et al., 2006). The perceived security of the website increases with each successful transaction. With greater perceived security of websites, there is greater confidence and trust in the public internet to communicate secure information with the e-commerce website. The public internet enhances the perception that the e-commerce website provides better security. Therefore, we propose that:

> H2: Increased perceived security of the e-commerce website positively influences attitude towards conducting e-commerce transactions over the public internet.

The research model, including control variables and the previously established relationship between consumer attitudes predicting consumer behavior intentions is illustrated in Figure 1 below.

RESEARCH MODEL

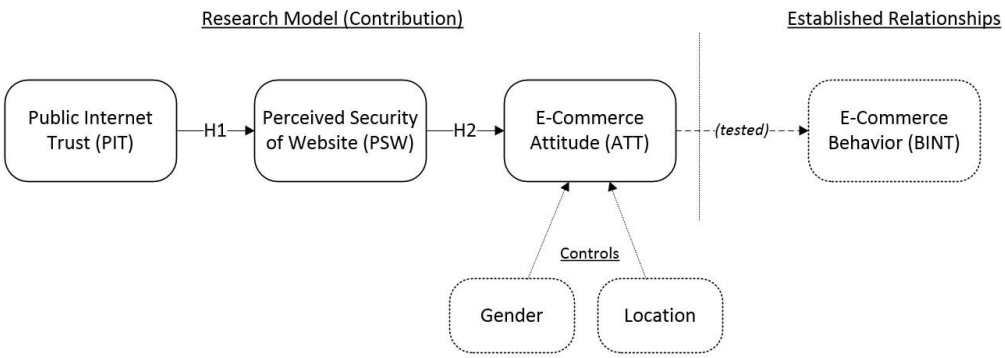

Figure 1. Research Model

METHODS

We constructed a survey instrument to investigate people's trust in public internet and its impact on people's attitude toward perceived security of websites and attitudes of e-commerce transactions. The survey initially primed participants with a brief scenario about the need to purchase a gift through an online retailer while having to use a free public internet connection. Following the scenario, participants completed a brief survey including measures related to the theorized constructs.

Participants and Procedure

We recruited student participants at two universities, one in the US and one in India, enrolled in classes related to information technology. There were 199 (N = 199) student participants with 82 located in the U.S. and the remaining 117 residing in India. The gender makeup of participants included 77 (38.7%) females and 122 males (61.3%). Largely the participants were ages 18-24 (87%), some were in the age range of 25-34 (12%), with the remaining between ages 45-54 (2%). This sample agrees with Smith's (2016) representation of the demographics of those who conduct online e-commerce transactions.

Construct Operationalization

We adapted scales from current literature to operationalize each construct from the research model. For brevity we've listed only a short description of each scale and its adaptation reference below.

Public Internet Trust (PIT): *adapted from Grabner-Kräuter and Faullant,2008*
Individual perceptions of trust in a free public internet connection in regards to the extent of what can and/or will happen when conducting an e-commerce transaction using free public internet connections.

Perceived Security of Website (PSW): *adapted from Roca et al., 2009*

Individual perceptions regarding the e-commerce website having appropriate technical capacity and capability to maintain consumer information in a secure and confidential manner when conducting an e-commerce transaction using free public internet connections.

E-commerce Attitude (ATT): *adapted from Grabner-Kräuter and Faullant, 2008*
Individual attitudes toward conducting e-commerce transactions over free public internet connections

E-commerce Behavioral Intention (BINT): *adapted from Venkatesh et al., 2012*

Individual intended behavior toward conducting e-commerce transactions over free public internet connections (common antecedent of attitude).

RESULTS

Descriptive Statistics and Reliability

To evaluate the results of the participant responses, we first examined each construct's reliability, mean, standard deviation and inter-correlation (see Table 1). The analysis indicated a significant correlation between all constructs and all scales achieved

and acceptable levels of reliability with a Cronbach's alpha α > .70 (Mackenzie et al., 2011). Furthermore, the average variance extracted (AVE) was examined to determine appropriate convergent validity of all indicators. All constructs achieved an AVE higher than .50, a preferred level to ensure the indicators account for the majority of the variance in their respective constructs (Mackenzie et al., 2011).

Variable	**1**	**2**	**3**	**4**	**M**	**SD**	**α**
1. Public Internet Trust (PIT)	[.57]	-	-	-	3.70	1.20	.74
2. Perceived Security of Website (PSW)	.31**	[.79]	-	-	4.76	1.27	.91
3. e-commerce Attitude (ATT)	.61**	.26**	[.90]	-	3.24	1.56	.94
4. e-commerce Behavior (BINT)	.65**	.25**	.82**	[.82]	3.53	1.48	.89
Note: N = 199, *ρ < .05, **ρ < .01, Dependent Variable = e-commerce Attitude, e-commerce Behavior is previously established, Controls: Gender and Location, Average Variance Extracted is denoted in [ ].							

Table 1: Means, Standard Deviations, Reliability, AVE, and Inter-Correlations among Variables

Hypotheses Testing

To test the hypotheses, we constructed an SEM-PLS model using Smart PLS to evaluate the relationships between constructs (See Figure 2). The PLS algorithm was applied to determine the factor loading of paths and bootstrapping, with 500 subsamples, was performed to test the statistical significance of each path coefficient. The paths between PIT / PSW and PSW / ATT were found significant ($\rho < .001$) giving support to H1 and H2. Furthermore, to confirm the relationship between ATT and BINT, the path model also shows this path as significant ($\rho < .001$). Additionally, the control variable for gender was not significant, however we did find the control variable of location have a significant path ($\rho < .001$).

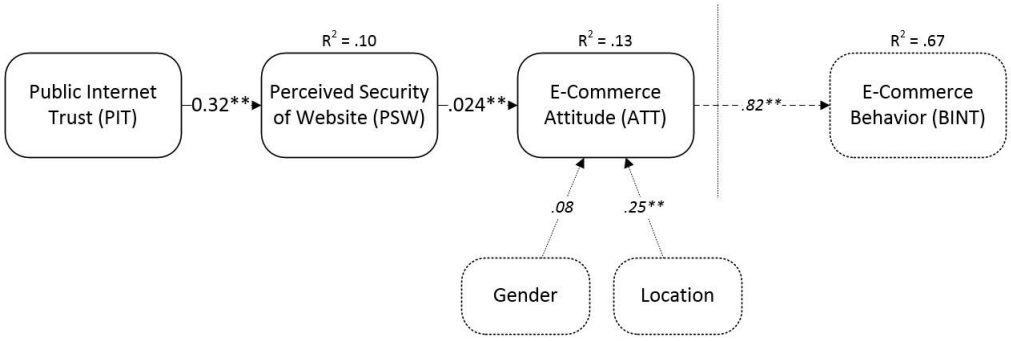

Figure 2. PLS Model - Results

DISCUSSION

The findings from the analysis suggest there is an impact of free public internet on consumer perceptions of website security, indicated by the significant relationship between public internet trust (PIT) and the perceive security of website (PSW). Our earlier discussion provides argument for this reasoning, as people view the trust in a public internet channel to perform in commutating information, both reliably and securely. Should the connection to an e-commerce website be compromised, it also threatens the perceived security of the website. The perception of website security also affects a person's attitude toward conducting e-commerce transactions on websites through free public internet as suggested by the significant relationship of PSW and their attitude in conducting an e-commerce transaction (ATT). These findings lead toward the need to investigate how consumers trust in free public internet dampens the likeliness people will conduct e-commerce transactions when they perceive internet channels as insecure.

CONCLUSION

In summary, this study provides researchers a direction when investigating another link in the e-commerce chain by looking toward public internet channels as a potential factor in consumer behaviors. Furthermore, this work can help practitioners to understand the impact weak public internet can have on their e-commerce websites. This can spur extended conversations on how to improve consumer trust in public internet to benefit consumer's perceptions of security of e-commerce websites.

REFERENCES

1. Byrd, C. (2011). Unsafe at any SSID. *ISSA Journal*, 9(3), 12-17.
2. Carlos Roca, J., José García, J., & José de la Vega, J. (2009). The importance of perceived trust, security and privacy in online trading systems. *Information Management & Computer Security*, 17(2), 96-113.
3. Chang, HsinHsin, and Su Wen Chen. "Consumer perception of interface quality, security, and loyalty in electronic commerce." *Information & management* 46.7 (2009): 411-417.
4. Chellappa, R. K., & Pavlou, P. A. (2002). Perceived information security, financial liability and consumer trust in electronic commerce transactions. *Logistics Information Management*, 15(5/6), 358-368.
5. Chellappa, Ramnath K., and Paul A. Pavlou. "Perceived information security, financial liability and consumer trust in electronic commerce transactions." Logistics Information Management 15.5/6 (2002): 358-368.
6. Cheng, T. E., Lam, D. Y., & Yeung, A. C. (2006). Adoption of internet banking: an empirical study in Hong Kong. *Decision Support Systems*, 42(3), 1558-1572.
7. Cheng, TC Edwin, David YC Lam, and Andy CL Yeung. "Adoption of internet banking: an empirical study in Hong Kong." *Decision support systems* 42.3 (2006): 1558-1572.
8. Chenoweth, T., Minch, R., & Tabor, S. (2010). Wireless insecurity. *Communications of the ACM*. ACM, 53(2), 134.
9. Corritore, C. L., Kracher, B., & Wiedenbeck, S. (2003). On-line trust: concepts, evolving themes, a model. *International Journal of Human-Computer Studies*, 58(6), 737-758.
10. D. Gefen, E. Karahanna, D.W. Straub, Trust and TAM in online shopping: an integrated model, MIS Quarterly 27 (2003) 51–90.
11. Ferreira, A., Huynen, J., Koenig, V., & Lenzini, G. (2014). Socio-technical Security Analysis of Wireless Hotspots. Lecture Notes in Computer Science Human Aspects of Information Security, *Privacy, and Trust*, 306-317.
12. Forbes. (2016). *What Are The Risks When Using Public Wi-Fi? Forbes.com*. Retrieved 19 December 2016, from http://www.forbes.com/sites/quora/2015/05/06/what-are-the-risks-when-using-public-wi-fi/#36d455d63f2c
13. Gefen, D., Karahanna, E., & Straub, D. W. (2003). Trust and TAM in online shopping: an integrated model. *MIS Quarterly*, 27(1), 51-90.
14. Grabner-Kräuter, S., & Faullant, R. (2008). Consumer acceptance of internet banking: The influence of internet trust. *International Journal of Bank Marketing International Journal of Bank Marketing*, 26(7), 483-504.
15. Hartono, E., Holsapple, C. W., Kim, K. Y., Na, K. S., & Simpson, J. T. (2014). Measuring perceived security in B2C electronic commerce website usage: A re-specification and validation. *Decision Support Systems*, 62, 11-21.
16. Hasan, B. (2010). Exploring gender differences in online shopping attitude. *Computers in Human Behavior*, 26(4), 597-601.
17. Jarvenpaas, Tractinsky et al. (2000) Consumer trust in an internet store. Information Technology & Management 1(1), 45–71.
18. Kalakota, R. and Whinston, A.B. (1997), *Electronic Commerce: A Manager's Guide*, Addison Wesley, Reading, MA.
19. Klasnja, P., Consolvo, S., Jung, J., Greenstein, B. M., LeGrand, L., Powledge, P., &Wetherall, D. (2009, April). When I am on Wi-Fi, I am fearless: privacy concerns & practices in everyday Wi-Fi use. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 1993-2002).
20. LaRose, R., &Rifon, N. J. (2007). Promoting i-safety: Effects of privacy warnings and privacy seals on risk assessment and online privacy behavior. *Journal of Consumer Affairs*, 41(1), 127-149.
21. Lee Jr, J., Warkentin, M., & Johnston, A. C. (2016). A Broader View of Perceived Risk during Internet Transactions. *Communications of the Association for Information Systems*, 38(1), 8.

22. Liu, C., Marchewka, J. T., Lu, J., & Yu, C. (2005). Beyond concern—a privacy-trust-behavioral intention model of electronic commerce. *Information & Management*, 42(2), 289-304.
23. MacKenzie, S. B., Podsakoff, P. M., & Podsakoff, N. P. (2011). Construct measurement and validation procedures in MIS and behavioral research: Integrating new and existing techniques. *MIS Quarterly*, 35(2), 293-334.
24. Marchany, R. C., & Tront, J. G. (2002). E-commerce security issues. In System Sciences, 2002. *HICSS. Proceedings of the 35th Annual Hawaii International Conference on System Sciences* (pp. 2500-2508). IEEE.
25. Mukherjee, A., &Nath, P. (2007). Role of electronic trust in online retailing. *European Journal of Marketing*, 41(9/10), 1173-1202.
26. Palvia, P. (2009). The role of trust in e-commerce relational exchange: A unified model. Information & Management, 46(4), 213-220.
27. Pennington, R., Wikox, H. D., & Grover, V. (2003–2004). The role of system trust in business-to consumer transactions. *Journal of Management Information Systems*, 20(3), 197–226.
28. Pullen, J. (2016). *Do This One Thing to Stay Safe On Public Wi-Fi. TIME.com*. Retrieved 19 December 2016, from http://time.com/4258958/wi-fi-security/
29. Ratnasingham, P. (1998). Internet-based EDI trust and security. *Information Management & Computer Security*, 6(1), 33-39.
30. Riquelme, I. P., & Román, S. (2014). Is the influence of privacy and security on online trust the same for all type of consumers? *Electronic Markets Electron Markets*, 24(2), 135-149.
31. Rotchanakitumnuai, S., & Speece, M. (2003). Barriers to Internet banking adoption: a qualitative study among corporate customers in Thailand. *International Journal of Bank Marketing*, 21(6/7), 312-323.
32. Salam, A. F., Rao, H. R., & Pegels, C. C. (2003). Consumer-perceived risk in e-commerce transactions. *Communications of the ACM*, 46(12), 325-331.
33. Salisbury, R. P., Pearson, A., & Miller, D. W. (2001). Identifying barriers that keep shoppers off the World Wide Web: developing a scale of perceived web security. *Industrial Management & Data Systems*, 101(4), 165e176.
34. Shankar, V., Urban, G. L., & Sultan, F. (2002). Online trust: a stakeholder perspective, concepts, implications, and future directions. *The Journal of Strategic Information Systems*, 11(3), 325-344.
35. Smith, C. (2016). The surprising facts about who shops online and on mobile. *Business Insider*. Retrieved 7 November 2016, from http://www.businessinsider.com/the-surprising-demographics-of-who-shops-online-and-on-mobile-2014-6
36. Venkatesh, V., Thong, J. Y., & Xu, X. (2012). Consumer acceptance and use of information technology: extending the unified theory of acceptance and use of technology. *MIS Quarterly*, 36(1), 157–178.
37. Zhou, L., Dai, L., & Zhang, D. (2007). Online shopping acceptance model-A critical survey of consumer factors in online shopping. *Journal of Electronic Commerce Research*, 8(1), 41.