Connecting to Unfamiliar Wi-Fi Hotspots : A Risk Taking Perspective

Research-in-Progress

Hoon S. Choi
University of Texas at San Antonio
hoonseok.choi@utsa.edu

Darrell Carpenter
University of Texas at San Antonio
darrell.carpenter@utsa.edu

ABSTRACT

Public Wi-Fi provides a convenient, cost-effective means for network connectivity in areas where wired infrastructure would be impractical. However, the use of multiple access points and radio wave transmissions present formidable challenges to providing a secure platform. Considering the rapid growth in Wi-Fi hotspot deployments and their potential vulnerabilities, the damage from these malicious activities could be substantial. While organizations deploying hotspots have great control over the security posture of the Wi-Fi network, the consumer has little insight into the risk associated with a particular system. Despite widespread knowledge of potential vulnerabilities related to public Wi-Fi, many people still connect to unfamiliar hotspots. We explore user perceptions of public Wi-Fi risks and benefits when making a connection decision. We develop a public Wi-Fi connection calculus model based on the theoretical foundations of motivational determinants of risk taking behavior theory, technology threat avoidance theory, and the extended privacy calculus model.

Keywords

Wi-Fi, wireless internet, public Wi-Fi, hotspot, risk taking behavior, technology threat avoidance theory

INTRODUCTION

Wi-Fi is an abbreviation of "wireless fidelity" and the commercial name for the IEEE 802.11 family of wireless Ethernet standards (Aime et al. 2007; Lehr et al. 2003). It provides wireless connections using high frequency radio signals to transmit and receive data within a limited range of a base station (Al-Alawi 2006; Egan et al. 2007). In addition, it generally provides data transmission speeds similar to cable modem-based Internet connections (Kabir et al. 2012).

Because of its convenience and speed, Wi-Fi has become popular with both business and private users since it was introduced in 1997 (Lemstra et al. 2009). According to the Wi-Fi Alliance, Wi-Fi is used by approximately 200 million households (CISCO 2012). It is also a popular method of providing network access in public places (Henry et al. 2002). In the United States, public Wi-Fi is available in nearly 70,000 businesses from small coffee shops to airports (Matarese 2011). While public Wi-Fi networks are already common in some venues, they are expected to grow in popularity in the near future. According to the Wireless Broadband Alliance (WBA) (2012), the number of Wi-Fi hotspots will increase to 5.8 million worldwide by 2015. A portion of this projected increase is attributable to major Wi-Fi deployment initiatives in large cities such as New York (WBA 2012), Chicago (Tribune 2012), Seoul(Independent 2011), and Beijing (CRJ 2012; ZDNet 2012). These cities and others are planning to provide free Wi-Fi access throughout their metropolitan areas.

Although public Wi-Fi networks generally provide simple, mobile, and potentially less expensive network connections than wired networks, they do not guarantee a secure network environment (Reddy et al. 2010). Communications between Wi-Fi hotspots and Internet devices can be easily hijacked through various hacking techniques (Leavitt 2011; CISCO 2012). Although there is no data available on losses stemming from compromised public Wi-Fi networks, security experts expect that approximately $1,000 worth of data can be stolen from one hacked computer (CBSNEWS 2010). When the number of Wi-Fi hotspots and their projected growth are considered, the potential damages from hacked public Wi-Fi networks are substantial for both individuals and businesses.

Research Problem: The popularity of public Wi-Fi hotspots and their inherent security vulnerabilities create a risk of substantial financial damages for both individuals and businesses.

According to experiments conducted by CBS News and the Guardian UK in 2010 and 2011, many people simply

connected to spoofed Wi-Fi hotspots established for the experiments. Moreover, a large portion of the people provided important personal information such as their mobile phone number, user ID and password, and even credit card numbers. This trend is somewhat perplexing given that most people are clearly aware of the potential dangers associated with using unfamiliar public Wi-Fi networks. According to the research conducted by the Identity Theft Resource Center (ITRC) (2012), although 79% of users were aware of the potential dangers in using public Wi-Fi, only 45% of those users reported concern about those issues.

Careless behavior by public Wi-Fi users is a primary factor in the overall security risk associated with these wireless networks. This behavior may lead to theft of personal information or breaches of information assets with potentially catastrophic consequences for both businesses and individuals. However, there are no prior studies exploring users' decisions to connect to unfamiliar Wi-Fi hotspots even though they are aware of their security vulnerabilities. Therefore, this research examines both motivations and risk perceptions to determine why people connect to unfamiliar Wi-Fi hotspots and relevant factors in their decision making.

Research Question: Why do people connect to unfamiliar public Wi-Fi hotspots despite their knowledge that it can lead to data loss, financial damage, and other potential problems?

In this research, a connection calculus for unfamiliar public Wi-Fi hotspots will be modeled based on established theoretical backgrounds such as motivational determinants of risk taking behavior theory, technology threat avoidance theory, and extended privacy calculus model.

LITERATURE REVIEW

Vulnerability of Public Wi-Fi networks

Many researchers have pointed out the vulnerabilities associated with public Wi-Fi, particularly those that are technical in nature. Nobles et al. claimed (2004) that security mechanisms of Wi-Fi are not sufficient to prevent malicious attacks, particularly in encryption and authentication processes. Aime et al. (2007) pointed out problems related to authentication, confidentiality, and privacy in Wi-Fi use. Reddy et al. (2010) demonstrated the vulnerability of Wi-Fi by cracking the encryption scheme of certain Wi-Fi devices. Gold (2011) argued that although Wi-Fi offers an array of encryption protocols including Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), and WPA2, all can be cracked to intercept transmissions between Wi-Fi hotspots and mobile devices.

In addition to these technical vulnerabilities, Leavitt (2011) suggested a scenario where hackers set up fake Wi-Fi hotspots and pretend to be a legitimate provider in order to obtain transmissions from mobile devices. These fake hotspots are referred to as Evil Twins. Because Wi-Fi access points use a Service Set Identifier (SSID) that is set locally to advertise their existence, it is extremely difficult to distinguish such fraudulent Wi-Fi hotspots from legitimate ones. When users unknowingly connect to a fraudulent access point they are subject to extreme risks of data loss. In several experiments conducted in London(Guardian 2011), Manhattan (CBSNEWS 2010), and Bristol (Kindberg et al. 2008), a large number of people either knowingly or unknowingly connected to fake Wi-Fi hotspots specifically deployed for the research experiments. These people often transmitted sensitive personal information including their user credentials, mobile phone numbers, and credit card information.

Risk Taking Behavior in Using Unfamiliar Public Wi-Fi

There is little empirical evidence examining the factors that lead users to connect to unfamiliar Wi-Fi hotspots despite their awareness of the risks. However, some studies have discussed potential motivations from a risk taking perspective. Klasnja et al. (2009) suggested that public Wi-Fi users believe they have enough protective measures on their systems to be secure. In reality, these protections are often inadequate, particularly with respect to mobile devices. Swanson et al. (2010) found that although the users were well aware of certain risks in using public Wi-Fi, they often do not believe the potential adverse effects will impact them. The two studies demonstrate that a person's risk taking perspective is strongly associated with the decision to use public Wi-Fi. Thus, the factors leading to risky behavior become important aspects of the connection calculus for unfamiliar public Wi-Fi use.

Risk Perception

Risk taking behavior has been extensively studied in various academic areas such as psychology, business, economics, and politics. Together, these studies suggest several variables that influence individual risk taking behavior. One widely discussed determinant is risk perception. Risk perception generally refers to "the intuitive risk judgments of individuals in the context of limited and uncertain information"(Messner et al. 2006). The degree of risk perception has a strong relationship with risk taking behavior in various contexts such as behaviors of adolescents (Mills et al. 2008), behavioral patterns of drug users (Connors 1992), characteristics of venture starters (Simon et al. 2000), decision making of business managers (Sitkin et al. 1995), and adoption of an online retailer (Chen et al. 2003). In the context of public Wi-Fi, users often perceive a low level of risk. This low degree of risk perception is expected to affect intention to use unfamiliar public Wi-Fi networks as noted in Hypothesis 1:

H1: Risk perception is negatively associated with intention to use unfamiliar public Wi-Fi networks.

Risk Propensity

Risk propensity refers to an individual's current tendency to take or avoid risks (Keil et al. 2000; Sitkin et al. 1995). Risk propensity has been associated with risk taking behavior in various studies (Fishburn 1977; Fu 1995; Kogan et al. 1964; MacCrimmon et al. 1990). In business disciplines, numerous studies have been conducted to clarify the determinants of risky decision making behavior. In a study of 101 graduate and undergraduate business students, Sitkin et al. (1995) illustrated that risk propensity is positively related to risky decision making behavior . MacCrimmon et al. (1990) analyzed socio economic data and business decisions of 509 executives and found that executives' risk propensity is a factor in risky decision making. Based on these studies, it is reasonable to expect that as users' risk propensity increases their intention to use unfamiliar public Wi-Fi systems will also increase.

H2: Risk propensity is positively associated with intention to use unfamiliar public Wi-Fi.

Perceived Avoidability

Perceived avoidability is another frequently considered determinant of risky decision making behavior. Perceived avoidability refers to the degree of individual's confidence in avoiding malicious attacks by using certain safeguarding measures (Liang et al. 2009). In the context of public Wi-Fi, users with confidence in safeguard software installed on their mobile devices may perceive the risk of connection to be lower than those without safeguard software. Thus, users employing safeguards will be less concerned about potential risks (Klasnja et al. 2009).

H3: Perceived avoidability is negatively associated with risk perceptions related to unfamiliar public Wi-Fi systems.

According to Liang et al. (2010), perceived avoidability is influenced by safeguard effectiveness, self-efficacy, and safeguard cost. Safeguard effectiveness describes the user's subjective beliefs regarding the effectiveness of safeguard measures in avoiding IT threats. Self-efficacy is defined as the level of user confidence in their ability to correctly use safeguard measures. Safeguard cost refers to a range of physical and cognitive efforts, such as time, money, and inconvenience, related to use of the safeguarding measures. In the context of public Wi-Fi, these three variables are expected to be significant predictors of user risk propensity. Therefore, when Wi-Fi users have high level of perceived safeguard effectiveness, high self-efficacy, and a low perception of safeguard cost, their perceptions of threat avoidability will be high.

H4: Safeguard effectiveness is positively associated with perceived avoidability in relation to unfamiliar public Wi-Fi systems.

H5: Self-efficacy is positively associated with perceived avoidability in relation to unfamiliar public Wi-Fi systems.

H6: Perceived cost is negatively associated with perceived avoidability in relation to unfamiliar public Wi-Fi systems.

Perceived Threat

In the cyber security realm, perceived threat refers to the degree of harm one may suffer from a malicious attack (Liang et al. 2010). Perceived threat is expected to be positively related to public Wi-Fi risk perceptions. For example, when a person believes using a public Wi-Fi hotspot could subject them to substantial harm, his or her overall risk perception will be high.

H7: Perceived threat is positively associated with risk perceptions related to unfamiliar public Wi-Fi systems.

Liang et al. (2010) also suggested that the overall perception of threat is determined by perceived severity and perceived susceptibility. Perceived severity is defined as the extent to which an individual believes negative impacts from a malicious event will be substantial. Perceived susceptibility refers to an individual's degree of belief that malicious attacks will negatively affect him or her (Liang et al. 2009). Based on these previous theoretical developments the following hypotheses are proffered:

H8: Perceived severity is positively associated with perceived threat in relation to unfamiliar public Wi-Fi systems.

H9: Perceived susceptibility is positively associated with perceived threat in relation to unfamiliar public Wi-Fi systems.

Outcome History

Outcome history is concerned with whether individual's previous risk related decisions have resulted in successful or unsuccessful outcomes (Sitkin et al. 1995). The impact of outcome history on the decision making process has been extensively studied in a variety of areas such as finance, organizational behavior, and software development. Weber and Milliman (1997) found that outcome feedback from previous investments clearly influenced the future decisions of stock investors. Byrne (2005) found that positive outcome history leads to higher risk propensity in financial product purchase behaviors. Therefore, outcome history is expected to be positively related to risk propensity for public Wi-Fi. Users who have suffered a previous data loss from malicious network activity will be less likely to use unfamiliar public Wi-Fi hotspots.

H10: Negative outcome history is associated with a low level of risk propensity in relation to unfamiliar public Wi-Fi systems.

Demographics: Age and Gender

The relationship between risk propensity and age has been studied in various areas. Nicholson et al. argued that old people tend to have lower levels of risk propensity than young people (2005). Deakin et al. (2004) found that the decisions made by older people tends to be slower and less risky than younger people in computer based gambling experiments. Grable (2000) demonstrated that older people have less risk taking tolerance in various financial situations. Accordingly, we expect younger subjects to exhibit a higher level of risk propensity than older subjects.

H11: Age is negatively associated with risk propensity related to unfamiliar public Wi-Fi systems.

Similar to the impact of age, prior studies have demonstrated that gender is related to risk taking behaviors in various domains. Powell and Ansic (1997) illustrated that females have a lower risk propensity than males in financial decision making, regardless of familiarity, costs, or ambiguity of situations. Zuckerman et al. (2000) found that males have substantially higher risk taking propensities in drug use, risky driving, and gambling. Dwyer et al. (2002) observed that female investors are less likely to take sizable risks when faced with uncertainty in mutual fund investment decisions. Harris et al. (2006) showed that women have a lower propensity toward risky decisions in gambling, recreation, and health areas. Based on these previous studies, males are expected to report a higher propensity for risk than females in regards to public Wi-Fi systems.

H12: Male users are more likely than females to engage in behavior with a high risk level when using unfamiliar public Wi-Fi systems.

Personality: Big Five (Neuroticism, Extraversion, Openness, Agreeableness, and Conscientiousness)

Personality is a well-studied factor in relation to risk taking behavior. Prior studies have demonstrated that the five personality traits (i.e., neuroticism, extraversion, openness, agreeableness, and conscientiousness) are highly important in explaining risk behavior. Nicholson et al. (2005) found that high level of extraversion and openness are positively associated with a high degree of risk propensity while neuroticism, agreeableness, and conscientiousness are negatively associated with risk propensity in a variety of situational settings such as recreation, health, career, and safety.

Weinstein and Martin (1969) found that extraversion is the most significant personality factor in relation to material risk taking. In this work material risk taking was distinguished from interpersonal risk taking to focus on the potential for material losses. Malec (1985) demonstrated that extroverted people are more likely to take risk and, consequently, more likely to suffer serious injuries in comparison to introverted people. Watson et al. (2004) found that people enjoying high risk sports tend to be more extroverted than the general population.

Openness is another critical predictor of risk taking behavior. Booth-Kewley and Vickers (1994) found that openness to experience is a statistically significant predictor of material risk taking behavior. Lauriola et al. (2001) showed that openness to experience is significantly related to risk taking propensity. Zhao et al. (2006) found that entrepreneurs are more open to new experiences than the general management population. Thus, in the context of public Wi-Fi, both extraversion and openness are expected to be positively associated with risk taking behavior.

H13a: Extraversion is positively associated with risk propensity in relation to unfamiliar public Wi-Fi systems.

H13b: Openness is positively associated with risk propensity in relation to unfamiliar public Wi-Fi systems.

Neuroticism, agreeableness, and conscientiousness are expected to be negatively associated with the level of risk propensity of using public Wi-Fi. Previous studies have illustrated an inverse relationship between these constructs and risk behavior. Trobst et al. (2002) found that agreeableness and conscientiousness are inversely associated with risk taking tendency in sexual behavior. Nicholson et al. argued that people with high risk taking propensity tend to have high levels of resilience (2005). Resilience has been shown to be positively related to low emotional sensitivity which serves as a proxy for low neuroticism.

H14a: Neuroticism is negatively associated with risk propensity related to unfamiliar public Wi-Fi systems.

H14b: Agreeableness is negatively associated with risk propensity related to unfamiliar public Wi-Fi systems.

H14c: Conscientiousness is negatively associated with risk propensity related to unfamiliar public Wi-Fi systems.

Personal Internet Interest and Incentive

In spite of the potential dangers of using public Wi-Fi, there are motivating factors that may lead some users to act in a careless manner. One motivating factor may be personal Internet interest. Personal Internet interest refers to the extent to which an individual has cognitive attraction to Internet interaction (Dinev et al. 2006). In their research, Dinev et al. found that personal Internet interest is significantly related to the willingness to provide personal information in transactions on the Internet. In the context of public Wi-Fi, personal Internet interest is expected to be positively associated with the intention to connect.

H15: Personal Internet interest is positively associated with intention to use unfamiliar public Wi-Fi systems.

Various incentives may also motivate individuals to use public Wi-Fi hotspots. Incentive is defined as the degree of attractiveness of a goal that is offered in a certain situation (Atkinson 1957). In the context of using public Wi-Fi, incentive would be the enjoyment or convenience experienced by using Internet services. According to research conducted by Klasnja et al. (2009), certain types of Internet applications were primarily concerned with entertainment and convenience, such as online shopping, photo sharing, social networking, and instant messaging. Alhakami et al. (1994) found that if people perceive a potential incentive to be large, they tend to make risky decisions. Therefore, if incentives such as entertainment and convenience are attractive in a particular situation, users are more likely to connect to unfamiliar public Wi-Fi systems.

H16: Incentive is positively associated with intention to use unfamiliar public Wi-Fi systems.

The research model depicting the hypothesized relationships is illustrated in Fig.1.

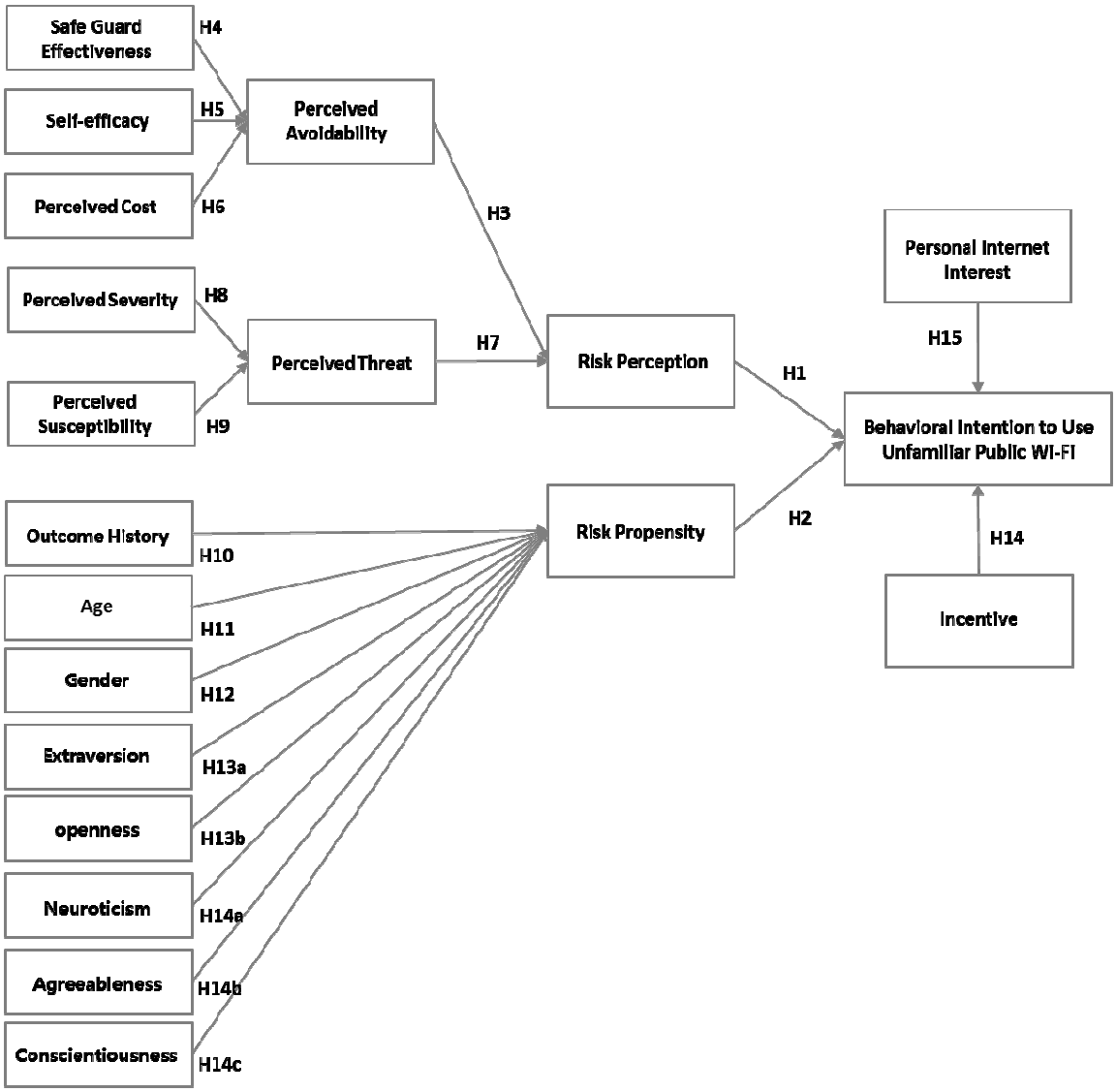

Fig 1. Research Model

RESEARCH METHODS

Measurement

Measurement items for this research will be primarily based on previously validated instruments (see Table 1). For variables related to risk propensity such as perceived avoidability, safe guard effectiveness, self-efficacy, perceived cost, perceived threat, perceived severity, and perceived susceptibility, the items will be based on Liang et al. (2010). Items related to outcome history and risk propensity will be adapted from Sitkin et al. (1995). Because the items from Sitkin et al. were developed for a managerial decision making instrument, they will be modified with appropriate contextual cues. Items for evaluating the five personality traits will be adapted from Costa and McRae's Five-Factor model (1992), which is among the most widely used instruments in evaluation of personal traits. Items for estimating personal Internet interest will be based on Dinev et al. (2006).

variables	Theoretical Background	Reference
Perceived avoidability	Technology Threat Avoidance Theory	Liang et al. (2009) Liang et al. (2010)
Safeguard effectiveness		
Self-efficacy		
Perceived cost		
Perceived threat		
Perceived severity		
Perceived susceptibility		
Personality	N-E-O-A-C Personality Traits Theory	Costa and McRae (1992)
Neuroticism		
Extraversion		
Openness		
Agreeableness		
Conscientiousness		
Personal Internet interest		Dinev et al. (2006).

Table.1. Measurement Items

Data Collection

In order to measure the relationships among variables in the research model, a survey with a hypothetical scenario will be administered. The scenario will be constructed to provide detailed information concerning the situation to derive respondents' decision or judgment as recommended by Alexander (Alexander et al. 1978). This data collection method has been widely used in security related studies in IS discipline, such as information systems misuse (Bulgurcu 2010), employees' perceptions of information security (Myyry et al. 2009), information policy violations of employees (Siponen et al. 2010), and piracy concerns of Internet users (Malhotra et al. 2004). The hypothetical scenario method appears well-suited for investigating the underlying determinants of intentions to use unfamiliar public Wi-Fi systems. In order to appropriately answer specific survey questions, the respondent must understand the detailed circumstances of the scenario. Accordingly, manipulation checks will be administered after the scenario is read and before the variable scale items are presented.

EXPECTED CONTRIBUTION

This research is expected to enrich the existing theory base on risk taking behavior by applying the concepts to an IS domain where the determinants of risk have been sparsely studied. The research will identify the driving factors that lead to risky outcome from the individual's connection calculus. This will inform future research aimed at modifying the outcome of the connection calculus to produce more desirable connection decisions. Similarly, the insights from this research may allow practitioners to focus their efforts on reducing motivations for risky behavior. Additionally, the insights gained will help practitioners identify groups of users who are more likely to engage in risky behavior so they may be targeted by organizational strategies. For example, if perceived threat is determined to be a significant factor, the potential damage from connecting to unfamiliar Wi-Fi hotspots can be emphasized in organizational training.

REFERENCE

1. Aime, M. D., Calandriello, G., and Lioy, A. 2007. "Dependability in Wireless Networks: Can We Rely on WiFi?," *IEEE SECURITY & PRIVACY*), pp 23-29.
2. Al-Alawi, A. I. 2006. "WiFi Technology: Future Market Challenges and Opportunities," *Journal of Computer Science* (2:1), pp 13-18.
3. Alexander, C. S., and Becker, H. J. 1978. "The Use of Vignettes in Survey Research," *The Public Opinion Quarterly* (42:1), pp 93-104.
4. Alhakami, A. S., and Slovic, P. 1994. "A Psychological Study of the Inverse Relationship Between Perceived Risk and Perceived Benefit," *Risk Analysis* (14:6), pp 1085-1096.
5. Atkinson, J. W. 1957. "Motivational determinants of risk-taking behavior," *Psychological Review [PsycARTICLES]* (64:6, Pt.1), pp 359-372.
6. Booth-Kewley, S., and Vickers, R. R. 1994. "Associations between Major Domains of Personality and Health Behavior," *Journal of Personality* (62:3), pp 281-298.
7. Bulgurcu, B. 2010. "Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness," *Women* (221:243), p 243.
8. Byrne, K. 2005. "How do consumers evaluate risk in financial products?," *Journal of Financial Services Marketing* (10:1), pp 21-36.
9. CBSNEWS 2010. "Dangers of Free Public Wifi," *CBSNEWS*).
10. Chen, R., and He, F. 2003. "Examination of brand knowledge, perceived risk and consumers' intention to adopt an online retailer," *Total Quality Management & Business Excellence* (14:6), p 677.
11. CISCO 2012. "The Future of Hotspots: Making Wi-Fi as Secure and Easy to Use as Cellular,").
12. Connors, M. M. 1992. "Risk perception, risk taking and risk management among intravenous drug users: Implications for AIDS prevention," *Social Science & Medicine* (34:6), pp 591-601.
13. Costa, P. T., and MacCrae, R. R. 1992. *Revised NEO Personality Inventory (NEO PI-R) and NEO Five-Factor Inventory (NEO FFI): Professional Manual*, (Psychological Assessment Resources.
14. CRJ 2012. "Free Wifi in Hangzhou,").
15. Deakin, J., Aitken, M., Robbins, T., and Sahakian, B. J. 2004. "Risk taking during decision-making in normal volunteers changes with age," *Journal of the International Neuropsychological Society* (10:04), pp 590-598.
16. Dinev, T., and Hart, P. 2006. "An Extended Privacy Calculus Model for E-Commerce Transactions," *Information Systems Research* (17:1), pp 61-80,100.
17. Dwyer, P. D., Gilkeson, J. H., and List, J. A. 2002. "Gender differences in revealed risk taking: evidence from mutual fund investors," *Economics Letters* (76:2), pp 151-158.
18. Egan, M. T., and Sandberg, W. S. 2007. "Auto Identification Technology and Its Impact on Patient Safety in the Operating Room of the Future," *Surgical Innovation* (14:1) March 1, 2007, pp 41-50.
19. Fishburn, P. C. 1977. "Mean-Risk Analysis with Risk Associated with Below-Target Returns," *The American Economic Review* (67:2), pp 116-126.
20. Fu, J. 1995. "071094 (E53, B70) Increased risk aversion and risky investment, University of Iowa, The Journal of Risk and Insurance, Vol. 60, nr. 3, 1993, pp. 494–501," *Insurance: Mathematics and Economics* (16:2), p 188.
21. Gold, S. 2011. "Cracking wireless networks," *Network Security* (2011:11), pp 14-18.
22. Grable, J. E. 2000. "Financial Risk Tolerance and Additional Factors That Affect Risk Taking in Everyday Money Matters," *Journal of Business and Psychology* (14:4), pp 625-630.
23. Guardian, T. 2011. "Wi-Fi security flaw for smartphones puts your credit cards at risk," *The Guardian*).
24. Harris, C. R., Jenkins, M., and Glaser, D. 2006. "Gender differences in risk assessment: Why do women take fewer risks than men?," *Judgment and Decision Making* (1:1), p 48.
25. Henry, P. S., and Hui, L. 2002. "WiFi: what's next?," *Communications Magazine, IEEE* (40:12), pp 66-72.
26. Independent, T. 2011. "Seoul to offer free wifi in public areas ").
27. ITRC 2012. "Almost 80% Believe Free Wi-Fi Can Lead to Identity Theft, Study Finds," *Private WiFi*).
28. Kabir, A. F. M. S., Khan, M. R. H., Haque, A. A. M. M., and Mamun, M. S. I. 2012. "WiMAX or Wi-Fi: The Best Suited Candidate Technology for Building Wireless Access Infrastructure," *Conference: ICLAN'2007, IEEE France*).
29. Keil, M., Wallace, L., Turk, D., Dixon-Randall, G., and Nulden, U. 2000. "An investigation of risk perception and risk propensity on the decision to continue a software development project," *Journal of Systems and Software* (53:2), pp 145-157.
30. Kindberg, T., O'Neill, E., Bevan, C., Kostakos, V., Fraser, D. S., and Jay, T. 2008. "Measuring Trust in Wi-Fi Hotspots," *CHI*).
31. Klasnja, P., Consolvo, S., Jung, J., Greenstein, B. M., LeGrand, L., Powledge, P., and Wetherall, D. 2009. ""When I am on Wi-Fi, I am fearless": privacy concerns & practices in eeryday Wi-Fi use," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ACM: Boston, MA, USA, pp. 1993-2002.
32. Kogan, N., and Wallach, M. A. 1964. *Risk taking: A study in cognition and personality*, (Holt, Rinehart & Winston: Oxford, England.

33. Lauriola, M., and Levin, I. P. 2001. "Personality traits and risky decision-making in a controlled experimental task: an exploratory study," *Personality and Individual Differences* (31:2), pp 215-226.
34. Leavitt, N. 2011. "Mobile Security: Finally a Serious Problem?," *Computer* (44:6), pp 11-14.
35. Lehr, W., and McKnight, L. W. 2003. "Wireless Internet access: 3G vs. WiFi?," *Telecommunications Policy* (27:5–6), pp 351-370.
36. Lemstra, W., and Hayes, V. 2009. "License-exempt: Wi-Fi complement to 3G," *Telematics and Informatics* (26:3), pp 227-239.
37. Liang, H., and Xue, Y. 2009. "AVOIDANCE OF INFORMATION TECHNOLOGY THREATS: A THEORETICAL PERSPECTIVE," *MIS Quarterly* (33:1), pp 71-90.
38. Liang, H., and Xue, Y. 2010. "Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective*," *Journal of the Association for Information Systems* (11:7), pp 394-413.
39. MacCrimmon, K. R., and Wehrung, D. A. 1990. "Characteristics of Risk Taking Executives," *Management Science* (36:4), pp 422-435.
40. Malec, J. 1985. "Personality factors associated with severe traumatic disability," *Rehabilitation Psychology* (30:3), pp 165-172.
41. Malhotra, N. K., Kim, S. S., and Agarwal, J. 2004. "Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model," *Information Systems Research* (15:4), pp 336-355.
42. Matarese, J. 2011. "How safe is free public Wi-Fi?," *News Channel 5*).
43. Mayer, R. C., Davis, J. H., and Schoorman, F. D. 1995. "An Integrative Model of Organizational Trust," *The Academy of Management Review* (20:3), pp 709-734.
44. Messner, F., and Meyer, V. 2006. "Flood damage, vulnerability and risk perception–challenges for flood damage research," *Flood risk management: Hazards, vulnerability and mitigation measures*), pp 149-167.
45. Mills, B., Reyna, V. F., and Estrada, S. 2008. "Explaining contradictory relations between risk perception and risk taking," *Psychological Science* (19:5), pp 429-433.
46. Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T., and Vance, A. 2009. "What levels of moral reasoning and values explain adherence to information security rules? An empirical study," *European Journal of Information Systems* (18:2), pp 126-139.
47. Nicholson, N., Soane, E., Fenton-O'Creevy, M., and Willman, P. 2005. "Personality and domain-specific risk taking," *Journal of Risk Research* (8:2) 2005/03/01, pp 157-176.
48. Nobles, P., and Horrocks, P. A. Year. "Vulnerability of IEEE802.11 WLANs to MAC laver DoS attacks," Secure Mobile Communications Forum: Exploring the Technical Challenges in Secure GSM and WLAN, 2004. The 2nd IEE (Ref. No. 2004/10660)2004, pp. 14/11-14/15.
49. Powell, M., and Ansic, D. 1997. "Gender differences in risk behaviour in financial decision-making: An experimental analysis," *Journal of Economic Psychology* (18:6), pp 605-628.
50. Reddy, S. V., Sai Ramani, K., Rijutha, K., Ali, S. M., and Reddy, C. P. Year. "Wireless hacking - a WiFi hack by cracking WEP," Education Technology and Computer (ICETC), 2010 2nd International Conference on2010, pp. V1-189-V181-193.
51. Simon, M., Houghton, S. M., and Aquino, K. 2000. "Cognitive biases, risk perception, and venture formation: How individuals decide to start companies," *Journal of business venturing* (15:2), pp 113-134.
52. Siponen, M., and Vance, A. 2010. "Neutralization: new insights into the problem of employee information systems security policy violations," *MIS Quarterly* (34:3), p 487.
53. Sitkin, S. B., and Weingart, L. R. 1995. "DETERMINANTS OF RISKY DECISION-MAKING BEHAVIOR: A TEST OF THE MEDIATING ROLE OF RISK PERCEPTIONS AND PROPENSITY," *Academy of Management Journal* (38:6), pp 1573-1592.
54. Swanson, C., Urner, R., and Lank, E. 2010. "Naïve Security in a Wi-Fi World," in *Trust Management IV,* M. Nishigaki, A. Jøsang, Y. Murayama and S. Marsh (eds.), Springer Berlin Heidelberg, pp. 32-47.
55. Tribune, C. 2012. "City plans free Wi-Fi in all parks, public spaces," *Chicago Tribune*).
56. Trobst, K. K., Herbst, J. H., Masters Iii, H. L., and Costa Jr, P. T. 2002. "Personality Pathways to Unsafe Sex: Personality, Condom Use, and HIV Risk Behaviors," *Journal of Research in Personality* (36:2), pp 117-133.
57. Watson, A. E., and Pulford, B. D. 2004. "PERSONALITY DIFFERENCES IN HIGH RISK SPORTS AMATEURS AND INSTRUCTORS," *Perceptual and Motor Skills* (99:1) 2004/08/01, pp 83-94.
58. WBA 2012. "WBA Wi-Fi Industry Report: Global Trends in Public Wi-Fi," *informa telecoms & media*).
59. Weber, E. U., and Milliman, R. A. 1997. "Perceived Risk Attitudes: Relating Risk Perception to Risky Choice," *Management Science* (43:2), pp 123-144.
60. Weinstein, E., and Martin, J. 1969. "GENERALITY OF WILLINGNESS TO TAKE RISKS," *Psychological Reports* (24:2) 1969/04/01, pp 499-501.
61. ZDNet 2012. "Beijing opens up more free Wi-Fi hotspots,").
62. Zhao, H., and Seibert, S. E. 2006. "The Big Five personality dimensions and entrepreneurial status: A meta-analytical review," *Journal of Applied Psychology* (91:2), pp 259-271.
63. Zuckerman, M., and Kuhlman, D. M. 2000. "Personality and Risk-Taking: Common Bisocial Factors," *Journal of*

Personality (68:6), pp 999-1029.