Journal of Internet Banking and Commerce

An open access Internet journal (http://www.arraydev.com/commerce/jibc/)

Journal of Internet Banking and Commerce, August 2013, vol. 18, no.2
(*http://www.arraydev.com/commerce/jibc/*)

The Impact of Identity Theft on Perceived Security and Trusting E-Commerce

ZAKARIA SALEH, PhD
Associate Professor, IT program, American Intercontinental University, USA
Postal Address: **AIU,** Schaumburg, IL 60173, USA
Email: **Zak.Saleh@aiuonline.edu**

Dr. Zakaria Saleh is an Associate Professor in IT at the American Intercontinental University, USA. His work experience ranged for simply providing technical support and non-conformance resolutions for a "Compaq Computers" PC configuration center, to working on the design and development of electronic control systems in the Automotive Industry, where he has contributed to the introduction of the M2M (Machine to Machine) Communication Systems. Prior to joining academia, he was working as a Project Engineer, at Case Corporation, an International Designer and Manufacturer of Agricultural and Construction Equipment, located in the USA. He was the lead engineer to work on the design and development of web based Fleet Management System.

Abstract

The research into consumer choices and acceptance of new products and services is normally discussed within the framework of diffusion of innovations and has traditionally relied on identifying consumer characteristics while focusing on the characteristics of innovations. The purpose of this study is to examine the impact of Identity theft on the perceived level of security mad trusting E-Commerce.

Keywords: **E-Commerce; Identity Theft; Internet Security; Risk**

INTRODUCTION

The enormous growth of Internet technology has made various resources on the Web instantly accessible to users. E-commerce has become a very important technological advancement for businesses in changing business practices (Brodie et al, 2007; Gonza´lez et al, 2008). The business organizations have also developed strategies to use the technology and expand their customer base and implement Electronic commerce (e-commerce) to deliver their products or services to the market through their ability to organize and maintain a business network. With any information technology, such online selling of products and services, ensuring transaction security is vital. However, measuring the security perceived by consumers usually involves some type of financial, performance, or social risks, where financial risk is not just the risk of losing money. In fact, Identity theft due to poor security measures could affect consumers' credit ratings or bank balances.

IDENTITY THEFT , INTERNET SECURITY, AND E-COMMERCE

While recent advancements in computer processing makes it easier for businesses and consumers to reach each other, they can also make suitable grounds for an impostor to obtain personal identifying information and then commit a crime known as Identity theft.

Identity theft is a one of the fastest growing crimes in which a criminal obtains key pieces of personal information in order to use it for own personal gain. Microsoft (2012) extends the definition of identity theft to be any kind of fraud that results in the loss of personal data, such as passwords, user names, banking information, or credit card numbers. Identity theft techniques can range from unsophisticated, such as mail theft to sophisticated tricks in which a pretender adopts somebody else's identity to gain access to their assets.

Identity theft is not new, and there have always been frauds who would use someone else's personal information such as name, social insurance number (SIN), credit card number or other identifying information to carry out fraudulent activities. However, technology, mainly the Internet, facilitates more harming schemes that in many cases results in financial loses and in some cases the victims of identity may experience difficulty obtaining credit or restoring their name.

Moreover, the problems caused by many computer virus, which swept computer systems worldwide in many cases, the distributed denial of service attacks on many e-commerce sites in the United States and Europe, as well as the hacking into the government's Web sites demonstrates the security of the Internet. In some cases, the attacks resulted in disclosure of sensitive customer data, and in some instances they did substantial damage to user/company relations, and they have caused inconvenience and frustration for millions of Internet users and increased concerns about the trustworthiness of the Internet.

E-commerce is on track to account for 53 percent of all purchases by 2014, according to recent Forrester Research predictions. This represents positive growth, but when you put it into perspective based on the Internet's overall growth potential, it's only a 10 percent annual increase (Mulpuru and Hult, 2010).

An Internet Usage Statistics, that was published by Miniwatts Marketing Group (2011) shows that the worldwide Internet users in December of 2000 were “360,985,492”, and in December 2011 the number of users became “2,267,233,742” , with a growth of 528.1% (Miniwatts Marketing Group, 2011), (see table 1 for number of Internet users).

According to Hernández et al. (Hernández et al, 2010), more and more consumers buy groceries and other foodstuffs via the Internet, and thus sales volume has been growing for the past 5 years at greater than 25% per year compared with stagnant increase in the overall market for foodstuffs. Appearance of the web site influence trust in the site through perceived ease of use (Vance et al, 2008), the consumer decision process has dramatically changed, even over the relatively short period of time the Internet has been with us (Edelman, 2010). Buyers in electronic markets are more susceptible to the lemons problem, as there is more incentive for sellers to market poor quality goods (Kshetri, 2010).

According to James (James, 2010), consumers' security fears can be categorized in three ways: the fear of identity theft and fraud; a negative perception of the merchant's security practices; and hesitation during the checkout process. Although more Americans than ever are going online, more Americans than ever distrust the Internet according to Tenth Study by the Digital Future Project (USC, 2011). The reports finds high levels of concern about corporate intrusion in personal lives, where Sixty-eight percent of Internet users said they buy online, however, respondents continue to report high levels of concern about credit card security when or if buying online, a finding that has continued in all of the Digital Future studies. In addition, while large percentages of Internet users buy online, even larger percentages continue to use the Web as a reference service before purchasing from local business.

Table 1: World Internet Usage and Population Statistics (Miniwatts Marketing Group, 2011)

World Regions	Internet Users Dec. 31, 2000	Internet Users Dec. 31, 2011	Penetration (% Population)	Growth 2000-2011
Africa	4,514,400	139,875,242	13.5 %	2,988.4 %
Asia	114,304,000	1,016,799,076	26.2 %	789.6 %
Europe	105,096,093	500,723,686	61.3 %	376.4 %
Middle East	3,284,800	77,020,995	35.6 %	2,244.8 %
North America	108,096,800	273,067,546	78.6 %	152.6 %
Latin America / Carib.	18,068,919	235,819,740	39.5 %	1,205.1 %
Oceania / Australia	7,620,480	23,927,457	67.5 %	214.0 %
WORLD TOTAL	360,985,492	2,267,233,742	32.7 %	528.1 %

According to TowerGroup (2009), there are almost 600 million E-Commerce users worldwide with a project growth rate that far outpaces the other banking services of ATM, branch and contact centers. The number of E-Commerce users globally is increasing at a compound annual rate of 20% through 2012, the firm said.

The open, interconnected nature of the Internet, which makes it such a useful and powerful medium, also makes it vulnerable to a variety of attacks. In recent years, there have been a variety of types of cyber-attacks. In general, the most important that relate to E-Commerce are: Denial of service, Cookie switching, IP spoofing, and Web spoofing, and identity theft. The performance and reliability fall short of expectations for commercial-grade sites and applications, however, as the end-user experience is at the mercy of the unreliable Internet and its middle mile bottlenecks (Leighton, 2009). In order to thrive in tomorrow's banking environment, TowerGroup recommends that banks focus on bolstering their e-Commerce channel to not only fend off disintermediation by non-bank players, but also to position their websites as the financial center whenever the consumer goes online. Banks have historically been the financial focal point for consumers, and in order to maintain their role as dominant financial advisors, they must dedicate their resources to improving their e-Commerce channel so that customers turn to their website for all of their banking needs (TowerGroup Research, 2009).

HYPOTHESIS

Intentions to use the Internet for purchasing products or obtaining services are positive indications and necessitate that a customer visits a business website and then complete a transaction. While the first phase was all about individual choices and better value for consumers, the second phase of Internet commerce is being redefined by the social media revolution of the last decade (Barwise and Meehan, 2010).

H01: Internet users do not have a negative attitude towards E-Commerce.

The Internet has opened up a world of opportunities for organizations to enhance operating efficiency, reduce costs, improve communication, and improve information delivery. However, the Internet also provides an opportunity for an intruder to compromise personal data and uses them for own personal gain.

H02: The Perceived level of the Internet security is positively associated with the level of customers concern about Identity theft.

Securing the Internet, like any other fields of computers, is based on the principle of confidentiality and integrity. Internet security incidents can be costly to the businesses that sell or provide services online. Other consequential damages are loss of reputation and loss of customer trust.

H03: Perceived level of internet security is positively associated with trusting E-Commerce.

The introduction of electronic payment complicates the process of secure payments. To complicate matters, the Internet was never designed for protection. Conversations about the opportunities and vulnerability of E-Commerce are to be found in almost every trade

magazine and industry forum.

> H04: Computer technical competence is positively associated with the perceived level of E-Commerce security.

There is still debate over the definition of identity theft, and the lack of consensus on a definition makes measuring identity theft a challenge. In addition, Lack a clear picture of the extent of identity theft or have good information about the sources of personal information being used by identity thieves. People will not trust what they do not understand.

> H05: Clear understanding of the extent of identity theft, is positively associated with trusting E-Commerce

SURVEY DESIGN

A survey was designed to find out the perceptions of Internet users about Internet security, understanding of the extent of identity theft, and find out whether or not these perceptions and understanding have any effect on trusting E-Commerce

The study was conducted in August of 2012 by having shopping mall "visitors" take a survey in three different locations in the State of Illinois (in three different counties). Only participants who use the Internet were allowed to take the survey (to eliminate the bias of none-Internet users). A total of 217 responses were received and used for this study.

Of 217 Internet users, 128 of them were male and 89 were female. The majority of the participants were between the ages of 18 and 43 (178 participants). 144 participants indicated that their level of education was two to four years college, and 73 participants had high school or less. Most of the participants' computer skills fall between average and high (161 participants). The Majority of the participants indicated being confident accessing the Internet (191 participants), and the majority of the participants use the Internet for more than five hours a week (165 participants).

HYPOTHESIS TESTING

The First Hypothesis (H1): Our first hypothesis is that Internet users do not have a negative attitude towards E-Commerce. Testing this hypothesis, the mean attitude score is 5.2 in the scale of 1 to 7 where "1" stands for "extremely disagree" and "7" stands for "extremely agree". The standard deviation of the attitude score is 0.85. The median of the attitude score is 5.95. The distribution is fairly symmetric about the mean (see figure 1).

The independent variables were scaled between 1, indicating respondents strongly disagreed, and 7, indicating respondents strongly agreed. A score of 3.5 on this scale indicated a neutral value. Since 3.5 correspond to the neutral point, we formulate the following statistical hypothesis in order to test our first hypothesis:

Null hypothesis: The average attitude score is equal to 3.5.

Alternative hypothesis: The average attitude score is greater than 3.5.

Using a one-sample t-test, we find an extremely small P-value, less than 0.1% (t-value is 6.66), which means that we can reject the null hypothesis at 0.1%, a very significant level. The testing result indicates that Internet users do not have a negative attitude towards E-Commerce, and it is so at a very high degree of confidence (at least 99.9%).

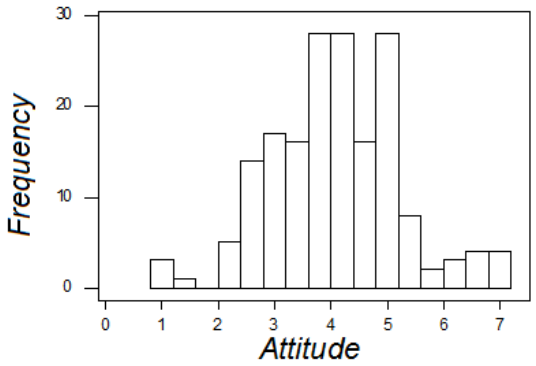

Figure 1. Histogram of Attitude Score

The Second Hypothesis (H02): We stated that the Perceived level of the Internet security is positively associated with the level of customers concern about Identity theft. Testing this hypothesis, the mean score for Internet security is 4.57 and the mean score for customers' concern about Identity theft is 4.27 in the scale of 1 to 7. The standard deviation of the Internet security score is 1.55 and the standard deviation of the customers concern about Identity theft score is 1.55. We tested to see if the slope significantly different from zero, and found that the P value is 0.349, which is considered not significant. We counted the number of runs, to see whether or not it indicates a linear model. The linearity evaluation is conducted by counting runs.

Table 2: Data of the Internet security and Identity Theft Concern slope

Parameter	*Best-fit* Value	*Standard* Error	*95% Coefficient Interval*	
			From	To
Slope	-0.0707	0.0754	-0.2186	0.077
Internet Security Intercept	4.6	0.36	3.89	5.31
Identity theft concern Intercept	65.1			

Small runs would indicate that the data deviate substantially from linearity. However, in the sample of 217 points, it is found that there are 83 points above the line, 94 below, and 92 runs. The P value is 0.693, which is considered not significant (see table 2 and figure 2). Based on the above testing result, we can reject the hypothesis.

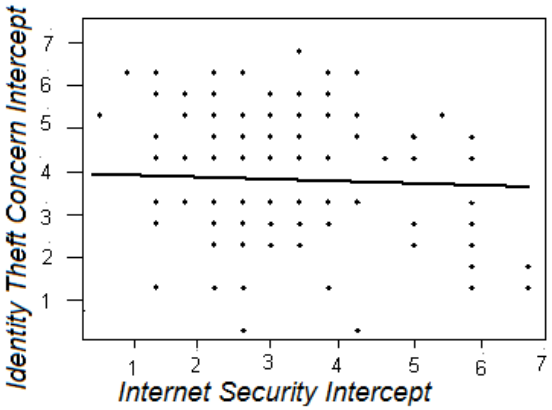

Figure 2. Linear Regression Plot of the perceived Internet security and the Identity Theft Concern

The Third Hypothesis (H03): We stated that the perceived level of internet security is positively associated with trusting E-Commerce. Testing that hypothesis, and at 95% confidence interval, we find that the correlation coefficient (R) = 0.447, and the R squared = 0.190. We also tested to see if the slope is significantly different from zero, and found that the P value is <0.0001, which is considered not extremely significant (See figure 3). Based on the above testing result, we can accept the hypothesis.

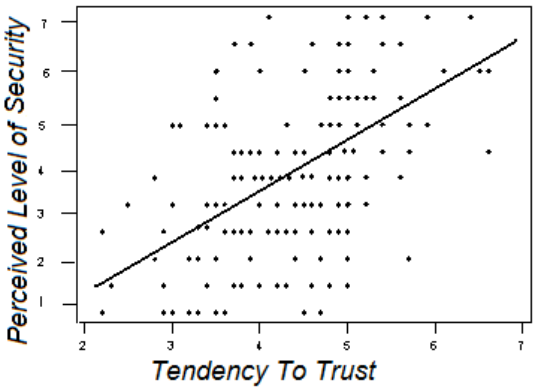

Figure 3. Linear Regression Plot of the perceived level of internet security and tendency to trust

The Fourth Hypothesis (H4): Our Fourth hypothesis states that Computer technical competence is positively associated with the perceived level of E-Commerce security. The Pearson correlation coefficient between the technical competences of Internet users the user's perceived level of E-Commerce security is 0.66, which indicates a fairly strong positive correlation. The P-value in testing the zero correlation is less than 0.1%, which means the correlation is very significant. Figure 4 presents the linear regression plot of the Pearson correlation coefficient. Based on the above testing result, we can accept the hypothesis.

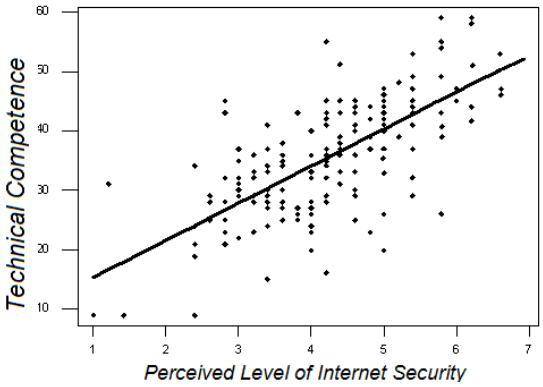

Figure 4. Linear regression plot of the technical competence of Internet users and the user's perceived level of E-Commerce Security

The Fourth Hypothesis (H5): We stated that the clear understanding of the extent of identity theft is positively associated with trusting E-Commerce. To seek the association between the users' tendency to trust E-Commerce and having clear understanding of the extent of identity theft, the correlation analysis was conducted. The Pearson correlation coefficient is found to be 0.209 and the corresponding P-value is 0.004 or 0.4%. This means the positive correlation between the two measurements is statistically significant though it is not strong. Figure 5 illustrates the users' tendency to trust E-Commerce and having clear understanding of the extent of identity theft.

Figure 5. Linear Regression Plot of Having Clear Understanding of the Extent of Identity Theft and Trusting E-Commerce.

ANALYSIS AND CONCLUSION

Consumers have changed their spending habits to adapt to this new economy. Shoppers are more selective and cautious about how they spend their money, and security apprehension still remains a hindrance to e-commerce (Mulpuru and Hult, 2010), and while Identity theft is not new, and there have always been frauds who would use someone else's personal identifying information to carry out fraudulent activities.

This study finds that Identity theft is one of the fastest growing types of fraud.

Table 3: Identity Theft Statistics for the years 2009–2011*

Report Year	Reported Identity Thefts	Total of all crimes	Percentage of All Crimes	Rank Among Crimes
2009	27,600	336,655	8.20%	4th
2010	50.43	303,809	16.60%	2nd
2011	68,190	314,246	21.70%	2nd

* Sources of raw data : The Internet Crime Complaint Center (IC3, 2009; IC3, 2010; IC3, 2011)

Analyzing the Incidents Crime Reports of The Internet Crime Complaint Center (IC3), for the calendar years 2009–2011 (table 3), we find that Identity Theft is on the rise, and has moved from being the fourth of the Top 5 Most Common IC3 Complaint Categories to become the second most reported crimes in 2011 (IC3, 2009; IC3, 2010; IC3, 2011). The analysis also indicates an increase of 35% over the year 2010 and 150% increase over the year 2009. In addition, analyzing the IRS, IPSU Identity Theft Report for the calendar years 2009–2011, reported 1,125,634 incidents (IRS, 2011). Comparing this number with 2009 and 2010 reported incidents, we find an increase of 155% over the year 2010 and 146% increase over the year 2009 (see table 4).

An interesting observation is that of all the complaints in the IC3 reports, only 36.9 percent reported financial loss, this data could be interpreted in different way, assuming the efficiency of prevention action or only considering that some complaints are only related to tentative of crime. What is interesting is that analyzing all complaints reported is helpful in identifying trends and building statistical reports on the crimes. Another interesting point to make is when looking at table 4, the number of incidents of identity theft is higher than the number of taxpayers. The fact is, some people had more than one incident of identity theft.

Table 4: Identity Theft Incidents for Calendar Years 2009–2011 (IRS, 2011)

Calendar	*Action Code 501*		*Action Code 506*		*Totals*	
Year	Taxpayers	Incidents	Taxpayers	Incidents	Taxpayers	Incidents
2009	60,048	90,542	194,031	365,911	254,079	456,453
2010	69,142	101,828	201,376	338,753	270,518	440,581
2011	87,322	110,750	553,730	1,014,884	641,052	1,125,634

Identity theft is obviously a complex problem. Organizations clearly need to do a better job at safeguarding the personal information entrusted to their care. The analysis of the data obtained from IC3 and IRS points to an explosion of identity theft.

In addition, the data collect by this study, indicates that consumers currently do not have a great deal of trust that the organizations holding their personal information are protecting them against identity theft. The participants believe that it is the merchant's responsibility to prevent identity theft during and after any online transaction. That suggests if any security issues occur while on the site or in the future, not only the blame will fall on the merchant, but also, it will impact future transactions.

The study finds that the participants agree that weak authentication and authorization is a significant E-commerce security risk for customers. This was recognized from the participants' answers on the questions of whether or not the website allows users to make multiple log-in attempts without locking the account (58% of the participants made multiple log-in attempts), and whether or not this would be a significant security risks (100% fully agreed).

The study does not find a significant correlation between Perceived level of the Internet security and the level of customers fear about becoming victims of Identity theft. Before the study was conducted, the expected outcome was that participants who believed that the internet is secures would have less or no fear of becoming victims of Identity theft than the participants who believe that the Internet is not secured enough. But we were getting mixed answers, and some were extreme (e.g. strongly agree that the Internet is secured and strongly agree that they could become victims of Identity theft).

However, when we found positive correlation between users' tendency to trust E-Commerce and having clear understanding of the extent of identity theft, we looked at the surveys of the participants who supported this expectations, and no mixed answers were found among those participants. Which suggest that there are people who have no trust in the system no matter how secured it may be, and there should be some kind of assurance done by merchants to gain the trust of those people. Trust is central to customer's merchant's relationships and it is crucial when it involves risk and uncertainty. Since the possibility exists for a third party to obtaining personal identifying information, this increases uncertainties, and therefore, the need for trust grows.

REFERENCES

Barwise, P. and Meehan, S. (2010). "The One Thing You Must Get Right When Building a Brand," Harvard Business Review, Vol. 88, No.12, pp 80-84.

Brodie RJ, Winklhofer H, Coviello NE. Johnston WJ (2007). "Is emarketing coming of age? An examination of the penetration of emarketing and firm performance", J. Interact. Mark. Vol 21 No 1, pp 2-21.

Edelman, D. C. (2010). "Branding in the Digital Age," Harvard Business Review, Vol. 88, No. 12, pp 62-69.

Gonza´lez ME, Dentiste MR, Rhonda MW (2008). "An alternative approach in service quality: an e-banking case study", Qual. Manage. J. 15 (1): 41.

Hernández, B., Jiménez, J., and Martín, M. J. (2010). "Customer Behavior In Electronic Commerce: The Moderating Effect Of E-Purchasing Experience," Journal of Business Research, Vol. 63, No. 9/10, pp 964-971.

IC3, (2009). 2009 Internet Crime Report. The Internet Crime Complaint Center publication

IC3, (2010). 2010 Internet Crime Report. The Internet Crime Complaint Center publication

IC3, (2011). 2011 Internet Crime Report. The Internet Crime Complaint Center publication

IRS (2011), IRSIPSU Identity Theft Report (Oct. 1, 2011);

James, S. (2010). What Security Fears Cost E-Commerce. E-Commerce Times, 04/01/2010 issue. Retrieved from WWW on August 1, 2012 at: http://www.ecommercetimes.com/story/69667.htmlIC3, (2009). 2009 Internet Crime

Kshetri, N.(2010). The Global Cyber-crime Industry: Economic, Institutional and Strategic Perspectives, Springer-Verlag: Berlin and Heidelberg, ISBN: 3642115217.

Leighton, T. (2009). "Improving Performance on the Internet". Communication of the ACM, Vol 52 No 2, pp 1-8

Microsoft (2012). What is identity theft? Microsoft Safety & Security Center. Retrieved from WWW on August 5, 2012 at: http://www.microsoft.com/security/default.aspx

Miniwatts Marketing Group (December 31, 2011), World Internet Usage Statistics, Retrieved from the WWW on April 22, 2012 at: http://www.internetworldstats.com/stats.htm

Mulpuru S. and Hult, P. (2010), "U.S. Online Retail Forecast, 2009 to 2014," Forrester Research, March 8, 2010

TowerGroup Research (2009). "The Summer Blockbuster: Moving Consumer E-Commerce from Supporting Cast to Lead Actor". TowerGroup Research Note, Retrieved from the WWW on May 10, 2012 at: http://www.towergroup.com/research/news/news.htm?newsId=5420.

USC (2011), 2011 Digital Future Report, University of Southern California Annual Report.

Vance, A., Elie-Dit-Cosaque, C., and Straub, D.W.(2008). "Examining Trust in Information Technology Artifacts: The Effects of System Quality and Culture," Journal of Management Information Systems, Vol. 24, No. 4. pp 73-100.