International Journal of Information Science and Management

The Behaviour and Perceptions of On-Line Consumers: Risk, Risk Perception and Trust

H. Jahankhani
University of East London
School of Computing and Technology
email: Hamid.jahankhani@uel.ac.uk

Abstract

The growth and the expansion of the Internet and the World Wide Web continue to impact society in new and amazing ways. The role of economic commerce has not been as dynamic as some predicted, but has still demonstrated remarkable success and tremendous potential. Any failure to meet some of the expectations may be explained in large part by questions and concerns surrounding existing methods of electronic commerce and of the Internet. A key negative perception centres on the security involved in Internet practice and electronic payment systems. Negative perceptions are then compounded and reinforced by massive media exposure of Internet security incidents. Many consumers still lack the necessary trust in on-line merchants and Internet security procedures and continue to use the Web to simply browse. The types of attack individuals face include confidence-trick or actual encounters calculated to extract bank or personal details, computer spyware that opens on accessing the Internet, enticing users with offers of non-existent free gifts while copying confidential files, and programmes that can infiltrate networks, operating within them undetected, ultimately causing them to crash. Social Engineering is one such method used by an attacker to get information. There are two main categories under which all social engineering attempts could be classified, computer or technology-based deception and human based deception. The technology-based approach is to deceive the user into believing that is interacting with the 'real' computer system (such as popup window, informing the user that the computer application has had a problem) and get the user to provide confidential information. The human approach is done through deception, by taking advantage of the victim's ignorance, and the natural human inclination to be helpful and liked. One of the most effective technology-based approach is a scam, called "phishing" as a form of identity theft. This is a technique used to gain personal information for the purposes of identity theft, using fraudulent e-mail messages that appear to come from legitimate businesses. These authentic-looking messages are designed to fool recipients into divulging personal data such as account numbers and passwords, credit card numbers and Social Security numbers. This paper provides an overview of electronic commerce and the impact of risk and trust on on-line shopping consumer behaviour. Due to the growth and potential of on-line shopping and the lack of academic-based research on Internet-related consumer behaviour, there is a tremendous need for impartial, academic investigation into the behaviour and perceptions of on-line consumers.

Keywords: Trust, Risk, E-commerce, online shopping, Internet shopping, impact, perceived risk, Social Engineering, Identity Theft, Phishing.

Introduction

The Internet and the WWW may be considered the ultimate business domain, perfectly designed for commercial exchange (McKnight, Choudhury, and Kacmar, 2002). Although, electronic commerce and the Internet shopping have been around for few years in the world of retail and sale, but, growth has been slower than some anticipated, although encouraging. In order to capitalise on the vast market potential of the Internet, there is a critical need for marketers to investigate consumer perceptions of on-line shopping. Concern exists over results of many surveys and studies of consumer demographics and user characteristics as a large part of existing research has been conducted by parties with "distinct commercial interest" in the results. A consistent theme throughout the research is a consumer concern over the security and risk involved in on-line shopping (Irakleous, Furnell, Dowland, and Papadaki, 2002). How ever successful, the use of the Internet has been held back by the lack of security, real or perceived. The future success of the internet as a viable mechanism for successful commerce depends not only on the development of safe and effective Internet Payment Systems (IPS), but also on the education of consumers and the alteration of the negative perceptions of the Internet security.

Today users are provided with a global telecommunication network, a virtual home entertainment centre convenient banking branch, a highly accessible library complete with vast stores of knowledge and information, a forum to share ideas and thoughts with anyone and everyone and a shopping outlet with an incomparable selection of products. The possibilities seem to be limited only by one's imagination.

While there is little dispute about the impressive growth in the number of host computers and users, actual Internet sales figures have fallen short of some original predictions. The failure to meet some expectations may be explained in large part by numerous aspects involving existing methods of electronic commerce and of the Internet itself. In the development phase of the basic underlying protocols, little thought was given to the issues of privacy and security because all information was freely provided to anyone interested.

A key negative perception centres on the security involved in Internet practice and electronic payment systems. The lack of an effective and trusted payment system that can be used in conjunction with on-line shopping has been a limiting factor in the growth of Internet sales (Sarkar and Cybulski, 2002). Consumers are hesitant to provide personal information, including credit card details, over the Internet because of concerns with privacy and fraud. Negative perceptions of questionable Internet security

procedures are then compounded and reinforced by massive media exposure of every Internet security incidents. Two area of consumer behaviour that would apply to this concern are risk and trust.

Online selling involves the buying and selling of products and services over the Internet. Online selling accounts for one of the major uses that the Internet as been put to over the years. It involves the disclosure of personal information by the customer and under the Data Protection acts; the service provider is under obligation to ensure the security of all information so gathered.

The online contract between a potential customer and a service provider does not have to follow a particular structure.

Its structure is dependent on the designer of the web pages for the service provider, it only obeys some specific rules most of which have been discussed.

The online contract, being a contractual obligation between both parties, must adhere to some or the entire following structural patterns;

- It must indicate clearly the quantity, value and/or description of products ordered. It should also indicate the full value of all services rendered.
- It should spell out clearly its accordance with relevant laws e.g. COPPA (Children's Online Privacy Protection Act) where the customer may be less than 13 years of age.
- It should get relevant personal data from the customer such as name, contact phone number, email address, delivery address, billing address, password if generated etc. It should ensure the transmission of the information through a Secured Sockets Layer (SSL) that encrypts the information.
- It should allow the customer to choose a billing option such as credit card and ensure the confirmation of the information thus given.
- It allows the customer to print a copy of such completed contract for record purposes.

This paper aims to provide an overview of the impact of risk and trust on on-line shopping consumer behaviour.

Globalisation VS. Localisation

The e-commerce environment in which organisations operate has come about as a result (to a large extent) of globalisation. There is an increasing interdependence of markets and industries, which has lead to the globalisation of the world economy. Blurred market boundaries, resulting in the changing barriers to entry have changed the internal and external structure of markets, as is seen in the EU. These factors have, further resulted in the need for mergers, alliances and acquisitions on a scale not seen before.

The Internet has also created a more dynamic supply chain for businesses. Business processes are now more modularised and the trend is to achieve a better vendor/consumer relationship. The Internet has allowed businesses to reach customers and suppliers in new areas. This global reach has also opened up the possibility for organisations to sell more of their products across all of the goods lifecycle. For example, raw material, finished goods, second hand goods and even scrap can now be sold.

Despite this obvious trend in the world economies (that of globalisation) there is a flip side to the coin. It is called localisation. Baker & McKenzie (2001) in an extensive report identified four main reasons why organisations localise their websites:

- To organise their market appearance and be accessible to buyers under a local top level domain name. For example; _.uk, _.de, _.fr, _.it and so on.
- To communicate with buyers/consumers in their local language.
- To meet the requirement of the local market.
- To meet the requirements of local laws and regulations.

Fifty percent of Western European executives identify a national or regional language and culture website, local presence, local fulfilment capability and the ability to launch across countries as important success factors.

Research work, has shown that US websites draw a lot of traffic, but very little trade from overseas. Most make no attempt to localise the contents of their website and international fulfilment is poor, this is mostly due to the homogeneous nature of the US environment. On the other hand, Europe's environment of distinct natural characteristics and laws is much more like the rest of the world. Europe's dot-coms are able to succeed in fighting their way through cultural, tax and regulatory obstacles, using their local knowledge to become long-term players. Having viewed both sides of the coin, one may now be tempted to ask the question "Which way do businesses go?" The answer is both, a little bit here and a little bit there. It is what business analysts call *"glocalisation"* meaning act global, but think local. With this, businesses would benefit from the best of both worlds.

Risk and Risk Perception

Over the course of an average day, an individual is faced with hundreds of situations in which a decision must be made. In most cases, there is no lengthy conscious deliberation of the pros and cons of each option. The individual simply assesses the situation, immediately weighs potential alternatives, makes a decision, and acts accordingly. The entire process may be as simple as whether or not to switch lanes while driving on the highway or whether to go to the bank at lunch or after work.

Risk includes an element of uncertainty and the consequences that are associated

with each course of action. Theoretically, the consumer will follow the option that is perceived to have the most favourable outcome. However, the probability of perceived outcome for a purchase situation is unknown. Each situation will also differ in the degree of perceived risk. The amount of risk that a consumer will experience is a function of two variables: the amount at stake (consequences) and the individuals feeling of subjective certainty of success or failure. Conceptually, something can only be gained if something else is risked. The amount at stake is that which will be lost if the situation is not successful or if the wrong choice is made. In a particular situation, the amount at stake is tied to the buying goals of the consumer (economic, physical, psychological etc). The inability to act, or the act of doing nothing, will carry its own set of consequences. The feeling of subjective certainty pertains to the likelihood of success that a consumer perceives in a situation. If the consumer feels very strongly that a purchase is the correct decision, the corresponding level of risk will be small. An extremely important concept in terms of risk perception is that risk is inherently subjective. The same purchase situation when presented to two different individuals may result in two very different levels of risk perception. The consumer can only react to the amount of risk she actually perceived and only to her subjective interpretation of that risk. Perceived risk is the result of subjective interpretation of objective criteria. In applying risk to situations involving technological considerations, Cunningham posed the question, "how safe is safe enough?" The answer seems to be a subjective one.

If the consumer perceives the level of risk associated with purchasing a product or service as too high, he/she will not complete the transaction. The consumer may initiate risk-reducing behaviours to account for the high levels of perceived risk. The consumer may either reduce the amount at stake or reduce the perceived uncertainty of the situation. Reducing the amount at stake may be accomplished by such acts as comparison shopping, trying a product sample, or purchasing insurance. The main way in which a consumer will reduce levels of uncertainty is by seeking more information. Sources of information sought can be obtained from past experiences of others published consumer reports and test studies, manufacturer's brochures, commercials and advertisements, news reports, on-line consumer groups and bulletin boards and newspapers and magazine stories.

Some research suggests that individuals will attempt to mediate levels of perceived risks in different ways. The author's research findings suggest that consumers who are highly "risk averse" perceive purchase situations more in terms of potential losses than gains.

Also theorized is that the probability of loss and the importance of loss are unique phenomena to individuals. This would help explain why individuals have subjective levels of risk perception. Research has demonstrated that high risk-perceivers engage in

greater amounts of risk- reducing strategies than low risk – perceivers (Prins,Ribbers, Van Tilbory, Veth, and Van Der Wees, 2002).

Risk as a Multidimensional Construct

Early studies on risk viewed risk as one-dimensional construct with the consumer exhibiting a consistent level of risk, regardless of the situation presented. Subsequent studies have attempted to separate risk into related, but independent components. The results are relatively consistent in identifying six components of risk, or predictor variables of the overall criterion variable of risk (Pope-Davis and Twing, 1991). These six components may vary in exact terminology, but relate to the same concepts:

- Financial risk: financial risk is associated with not receiving value for the amount paid or with paying more for a product than was necessary. Studies have demonstrated that financial, or economic, risk is consistently rated as having the greatest importance to consumers. The Financial cost of making a bad purchase decision is also the most common association made when the concept of risk is presented.
- Physical risk: Physical risk covers the potential for a service or product to pose a threat to the health or well-being of an individual as a result of its use or possession.
- Functional risk: Function risk is also known as performance risk; or quality risk. This covers the concern that a product or service will not meet performance expectations of the consumer or will not match the advertised product specifications. This type of risk would cover the fears of on-line consumers who are concerned that substandard products will be delivered.
- Psychological risk: Psychological risk deals with concerns that use or possession of the product will not match the personality of a consumer and how they perceive themselves. These are concerns that an individual has about himself or herself.
- Social risk: Similar to psychological risk, social risk instead covers the concerns resulting from others. Social risk describes the fear that a product or service will not convey the proper imagine to others or that might make the consumer self-conscious
- Time-loss risk: This type of risk is associated with the amount of time required to make a purchase, wait for a product to be delivered, or wasted as a result of being have to return or replace the product.

There are some disagreement in the literature as to the exact relationship of these six components and whether or not the six-component model sufficiently covers the criterion variable of risk Jacoby and Kapalan (1972) argue that each of the six components represent independent risk dimensions of their own. Other studies suggest that each component is related to the other components in varying degrees and each contributes some percentage to the whole in terms of the criterion variable of risk.

However, the exact percentage of contribution by each component will vary from

individual to individual and from purchase situation to purchase situation by each individual (Pope-Davis and Twing, 1991). Research findings have varied somewhat in their result in terms of explained variance by the six variable models. In Jacoby and Kapalan (1972) more than a third of the variance was accounted for. The varied results support the argument that the criterion risk model is lacking components, since the degree of unexplained variance is too great simply be attributed to measurement error.

Trust

Trust deals with belief, or willingness to believe, that one can reply on the goodness, strength and ability of somebody (the seller or the buyer) or something (Prins et al., 2002). No single factor may be more important to commercial ventures on the Internet than gaining and maintaining the trust of consumers. High levels of trust and positive electronic commerce experience increases the likelihood of consumers returning and establishing continuing relationships. Additionally, high trust fosters consumer willingness to increase the amount of information-sharing that enables electronic commerce to operate. The key issue is that developing positive trust relationships, which can prove difficult in normal business operations, is made even more difficult simply by the nature of the medium.

Trust, like risk, has been discussed for several decades and has been analyzed in such social science literatures as psychology, sociology, political science, anthropology, history, socio-biology and economic. With its application to the various fields, trust has been defined in many different ways. It has been described as the act of committing to an exchange before it is known how the other party will act (Coleman**,** 1990). The author describes it as a willingness of an individual to be vulnerable to another with the explanation that the other will perform a particular action. Deutsch in Lewicki and Bunker (1996) identifies three elements that must be present in a situation for trust to occur. First, there must be some degree of uncertainty about future course of actions. Second, the actions of the parties involved in the situation must have the ability to affect outcomes. Finally, the potential negative outcomes must be of greater magnitude than the potential positive outcomes. Consistent components throughout the trust literature are the elements of uncertainty of future outcomes, presence of risk in the situation, and the willingness of parties to act in accordance with the expected actions of the part of another.

In a purchase situation, the consumer must enter into the trusting relationship with the merchant. The author further points out the importance of the presence of risk factors by suggesting that trust is only relevant in a situation where the consumer has no control over the situation and stands to lose something of value. Stand another way, no trust is needed for a consumer to enter into action of there is nothing to lose and only

something to gain.

Zucker identifies three central sources of trust production (Zucker, 1986). Process-based trust is the trust that a consumer places in past experience. Brand loyalty and reputation are examples of process-based trust. Characteristic-based trust is associated with specific qualities about the product or company. Finally, institution-based trust encompasses the trust that a consumer would associate with formal institutions or certifications, such as the banking industry .The geographic distance that is possible between consumer and merchant and the large number of transactions that are likely make institutional-based trust of great importance to electronic commerce. The main factor seems to be that it allows the consumer to place trust in something with which they are familiar.

As a relationship builds, is it consumer/merchant or other, it progresses through three stages of trust: Calculus-based trust, knowledge-based trust, and identification-based trust (Lewicki, and Bunker, 1996; Ratnasingham, 1998; Zucker, 1986). Each level of trust is prerequisite to the next level in the relationship.

On-Line Shopping

Several of the risk factors described in the previous section can be easily applied to on-line shopping situations. An analysis of virtual transactions to this point indicates a high proportion of name brand items and low cost items being purchased (Pope-Davis and Twing, 1991). Frequently purchased items on the Internet to this point include travel services, newspaper and magazine publishing companies (Buck, 1996). This would seem to reflect the risk reduction methods of a) brand loyalty and b) reducing the amount at stake in a purchase situation by limiting cost. The risks associated with the inability to inspect merchandise, with difficulty in returning or exchanging merchandise, and with the shopping medium transfer easily as Internet Shopping is still a form of phone/mail order purchasing.

However, some elements of a virtual sales situation present unique risks to the traditional phone/mail order scenario. First; the on-line shopping involves the use of a new technology, both in the ordering process itself and in the security mechanisms used to secure the transmissions. The unfamiliarity of the technology and the uncertainly associated with anything new are important considerations of commercial Internet ventures. With lack of experience or available information and training, consumers may continue using the Web simply to collect information and not to purchase.

It has been theorized that the two most significant barriers to full scale electronic commerce are the security of Internet networks and applications and the security of commercial transactions conducted over the Internet (Ratnasingham, 1998). These security concerns are of extreme importance to commercial ventures in order to reduce

potential risks and enhance the level of trust on the part of consumers, (Bharania, 2005). With the increasing retail options available on the Net and the addition of encryption technologies, security has become more of a psychological issue than a financial or technological concern. In Electronic commerce, the ability of companies to reduce perceived risk and the establishment of trust between consumers and merchants is critical for consumers to engage in a virtual transaction beyond an initial purchase (Ratnasingham, 1998). Trust can be achieved or forfeited at several stages of a transaction. First, the quality of goods and services must be satisfactory. Second, the consumer must trust the manufacturer that the product or service will be delivered. Third, the consumer must trust the server and the manufacturer with the credit card transaction. Fourth, the consumer must trust the technology involved in establishing and maintaining security and privacy in the transaction. Fifth, the consumer must trust that if the product is damaged, defective, or unacceptable, the manufacturer will honour some form of return policy.

Social Engineering Attack on the Internet

Various authors have provided definitions, such as:

"Social engineering can be regarded as 'people hacking', basically its hacker jargon for soliciting unwitting participation from a person inside a company rather than breaking into the system independently", (Vigilante, 2007).

"Social engineering is a hack that uses brains instead of computer brawn. Hackers call data centres and pretend to be customers who have lost their password or show up at a site and simply wait for someone to hold a door open for them. Other forms of social engineering are not so obvious. Hackers have been known to create phoney websites, sweepstakes or questionnaires that ask users to enter a password", (Bannan, 2001).

"Social engineering is an art of utilising human behaviour to breach security without the participant even realising that they have been manipulated", (Gultai, 2003).

There are two main categories under which all social engineering attempts could be classified, computer or technology-based deception and human based deception. The technology-based approach is to deceive the user into believing that is interacting with the 'real' computer system (such as popup window, informing the user that the computer application has had a problem) and get the user to provide confidential information. The human approach is done through deception, by taking advantage of the victim's ignorance, and the natural human inclination to be helpful and liked.

"phishing" as a form of identity theft is a technique used to gain personal information for the purposes of identity theft, using fraudulent e-mail messages that appear to come from legitimate businesses. These authentic-looking messages are

designed to fool recipients into divulging personal data such as account numbers and passwords, credit card numbers and Social Security numbers. Phishing is a two time scam, first steals a company's identity and then use it to victimise consumers by stealing their credit identities. The term Phishing (also called spoofing.) comes from the fact that Internet scammers are using increasingly sophisticated lures as they "fish" for user's financial information and password data.

Phishing Technique

Phishing becomes the most commonly used social engineering attack due to the fact that it is quite easy to be carried out, no direct communication between hacker and victim is required (i.e. hacker doesn't need to phone their prey, pretending that they are a technical support staff, etc.). Sending mass-mails to thousands of potential victims increases the chance of getting someone hooked. There are usually 3 separate steps for this attacks to work these are;

1. Setting up a mimic website.
2. Sending out a convincingly fake e-mail, luring the users to that mimic site.
3. Getting information then redirect users to the real site.

In step 1, the hacker steals an organization's identity and creates a look-alike website. This can easily be done by viewing the targeted site's source code then copying all graphics and HTML lines from that real website. Due to this tactic, it would really be very hard for even an experienced user to spot the differences. On the mimic website, usually there will be a log-in form, prompting the user to enter secret personal data. Once the data is entered here, a server-side script will handle the submission, collecting the data and send it to the hacker, then redirect users to the real website so everything look unsuspicious.

The hardest part of phishing attack that challenges most hackers is in the second step. This does not mean it is technically hard, but grammatically it is! In this step, the hacker will make a convincingly fake e-mail which later will be sent by a "ghost" mailing program, enabling the hacker to fake the e-mail's source address.

The main purpose of this fake e-mail is to urge the users going to the mimic website and entering their data that hackers wanted to capture. Commonly employed tactics are asking users to response over emergency matters such as warning that customers need to log-in immediately or their accounts could be blocked; notifying that someone just sends the user some money and they need to log in now in order to get it (this usually is an effective trap to PayPal users), etc. Inside this fake e-mail, users often find a hyperlink, which once clicked, will open the mimic website so they can "*log in*". As discussed before, the easiest way to quickly identify a fake e-mail is not just by looking at the address source (since it can be altered to anything) but to check English grammar

in the e-mail. You may find this sounds surprising, however, 8 out of 10 scam e-mails have obvious grammar mistakes. Regardless of this, the trick still works.

In the last step, once a user has opened the mimic website and "*log in"*, their information will be handled by a server-side script. That information will later be sent to hacker via e-mail and user will be redirected to the real web site. However, the confidentiality of user's financial data or secret password has now been breached.

Conclusion

The primary purpose of this study was to examine consumers' perception on risk and trust in relation to on-line shopping, on-line merchants, and the underlying security procedures of the Internet.

The study has tackled the problem of identifying factors related to consumers' trust the consumer's privacy and security concerns are strongly associated with consumers' trust and purchase intention. Therefore, it is important that Internet retailers should make efforts to better incorporate trust-building mechanisms by focusing on the impact of consumers' privacy and security concerns with online purchases. Another implication from a marketing perspective is that customers who have a high degree of trust must have a high probability of becoming loyal customers in the near future.

Phishing becomes the most commonly used social engineering attack due to the fact that it is quite easy to be carried out, no direct communication between hacker and victim is required.

Phishing that replaces web browser address bar with malicious JavaScript fake is one of the most sophisticated one and has serious security implications for consumers. The key points are;

- Social engineering attacks have the highest success rate.
- Prevention includes educating people about the value of information and training them to protect it.
- Increasing people's awareness of how social engineers operate.

References

Baker & McKenzie (2001). *Doing E-commerce in Europe.* Retrieved September, 2007, from http://www.bakerinfo.com/BakerNet/default.htm

Bannan, K. J. (2001, January 1) *Internet World.*

Bharania, R. (2005). *Risk triage and prototyping in information security engagements*. USA: Cisco White paper.

Buck, S. P. (1996). Electronic commerce - would, could, and should you use current Internet payment mechanisms? *Internet Research*, 6, 5-18.

Coleman, J. (1990). *Foundations of social theory*. Harvard University Press.

Gulati, R. (2003). *The Threat of Social Engineering and your defense against it.* SANS Reading Room. GIAC Security Essentials Certification Practical Assignment, SANS Institute, USA.

Irakleous, I., Furnell, S. M., Dowland, P. S., & Papadaki, M. (2002). An experimental comparison of secret-based user authentication technologies. *Information Management & Computer Security, 10*(3), 100-108.

Jacoby, J., & Kaplan, L. (1972). The components of perceived risk. In M. Venkatesan (Ed.), *Advanced in consumer research*. Chicago: Association for consumer research.

Lewicki, R. J. and Bunker, B. B. (1996). Trust in relationships: A model of trust development and decline. In B. B. Bunker & J. Z. Rubin (Eds.), *Conflict, cooperation and justice: A tribute volume to Morton Deutsch*. San Francisco: Jossey Bass.

McKnight, D., Choudhury, V., & Kacmar, C. (2002, September). *Information Systems Research*, *13*(3).

Pope-Davis, D. B., & Twing, J. S. (1991). The effects of age, gender, and experience on measures of attitude regarding computers. *Computers in Human Behaviour, 7*(4), 333-339.

Sarkar, P. K., & Cybulski, J. L. (2002). *Understanding a product line of electronic business systems*. School of Information Systems, Deakin University.

Prins, J. E. J., Ribbers, P. M. A, Van Tilborg H, Veth, A. F. L., & Van Der Wees, J. (2002). *Trust in e-commerce*. Kluwer Law International.

Ratnasingham P. (1998). Internet-based EDI trust and security. *Information Management and Computer Security, 6*(1), 33-39.

Vigilante (2007). *Social Engineering*. Retrieved from www.vigilante.com/inetsecurity /socialengineering.htm

Zucker, L. G. (1986). Production of trust: Institutional sources of economic structure, 1840-1920. *Research in Organizational Behaviour, 8*, 53-111.