Online Trust: Strategies to build confidence from a business perspective

Fahri Karakaya \textsuperscript{1}, Suzanne Mello Stark\textsuperscript{2}

\textsuperscript{1} Professor of Marketing
Charlton College of Business, Department of Marketing
University of Massachusetts, Dartmouth, MA 02747-2300
\textsuperscript{2} Lecturer, Adjunct Assistant Professor
University of Rhode Island, Kingston, RI 02881

Abstract:
This paper examines the current problems associated with consumer trust in online purchasing. Research shows that trusting web sites is a major problem for consumers and distrust on web sites leads to a high number of consumers' abandoning shopping carts and therefore not purchasing products online. We identify the major reasons for online distrust and suggest ways of overcoming distrust in an online shopping environment by culminating previous research.

Keywords:
Online Trust, Business

Introduction
Trust is a major factor in doing business, and in people’s everyday lives. While there seems to be more than a single definition of trust, most of them have the common theme of knowing or believing that other parties involved in an interaction will not take advantage of the other party. Previous research indicates that there are various components of trust including “taking risk” [17], “cooperation” [28], “confidence” [3], and “loyalty” [11]; [24]. Since the e-Commerce, marketing and management literatures provide ample information on these topics, we will not reiterate these concepts here. Mayer et al. [28] developed a trust model in 1995 and indicated there is lack of research about trust in organizations. This model included three major factors that determine trust or trustworthiness such as ability, benevolence, and integrity. Other research that is more relevant to this study listed competence, predictability, benevolence, and integrity as trust related characteristics of a web site [29]. A more recent study indicated that web sites providing useful and accurate information and maintaining a reliable order fulfillment track record are perceived as having high levels of online trust [8].

Lauer and Deng [24] applied Mayer et al.’s [28] trust model to an Internet context. The findings suggested that consumers’ trust in a company was related to the perception of the company’s respect for customer privacy. Trust in turn was linked to increased customer loyalty. Some researchers indicate that online trust is as a key differentiator that determines the success or failure of many companies conducting their business over the Internet [47]; [44]. In a study, Elliott and Speck [10] found that trust is an important determinant of attitude toward retail web sites. Attitude toward a web site / company or product can serve as antecedent for trust [42]. An earlier study by
Lynch, Kent, and Srinivasan [27] indicated that trust positively led to increased intention to purchase online. This was later confirmed by other researchers (see for example: [7]; [25]; [42]; [43].

Casaló, Flavián and Guinalíu [7] added web site usability, company reputation, consumer satisfaction, perceived privacy, and security policy of websites as important items that influence online trust. According to Lauer and Deng [24] online trust could be enhanced through two complementary approaches: secured information technology and trusted business practices. The study conducted in 2007 focused on one important business practice; building online trust through a firm’s behavior with respect to privacy and found that consumers’ trust in a company is closely related to perception of the company’s respect for customer privacy. However, the study mentioned did not deal with the use of information technology in building and improving online trust. In this research, we add elaborate on the use of information technology in order to create and develop a secure shopping environment.

Wang et al. [48], Reicheld and Schefter (2000) argued that price is not the most important factor in purchasing online, but trust is. Indeed, earlier research shows that trust is an important variable that influences intentions for online transactions , [15]; [26]. These researchers also expanded the components of online trust by including the following: trustworthy interactions with customers at every step of the online purchasing process such as need recognition, information search, evaluation, negotiation and selection, purchase, payment and delivery, and after-purchase service and evaluation. The need for trust in an online environment increases because of the transaction complexity that is created by computer-mediated interaction [30].

Karakaya [19] indicates that customers’ perception of web sites being secure is crucial in allowing customers to complete their online transactions and keeping them loyal. Cyber security has received much attention in popular media because cyber-attacks on computer systems continue to grow. For example, Trembly [45] reports that there were 12,805 cyber-attacks against 5,000 targets over a three-week period. According to the recently released Norton Cyber Crime Report for 2011, 431 million adults worldwide were victims of cyber crime in 2010. The total cost of those crimes amounts to some $114 billion. Similarly, the Symantec Inc [40], 2011 report indicates that the total cost of cyber crime to online adults in 24 countries was $388 billion. These statistics are alarming and impact consumers’ online shopping behavior as well as online merchants’ taking action against cyber-crime.

Recent statistical data indicates that in 2012, shopping cart abandonment rates hit all time high, 72.31 percent compared to 59.8% in 2006 [5]. Surveys show almost three quarters of visitors leave sites when asked for what they believe is unjustified personal information [39]. Due to improvements in technology and time the ecommerce has been around, one would expect the shopping cart abandonment rates to decline. While there may be a number of reasons for shopping cart abandonments, we think trust on a web site is one of the most important reasons. With this in mind, we attempt to examine the “online trust” issue by first identifying the reasons of distrust and then offering some solutions to build and strengthen online trust for e-tailers.

**Reasons for Distrust on Online Shopping**
Information Privacy

We have seen many data breaches in the past where consumers’ e-mail addresses, credit card numbers, and other private information had been compromised. As a result of this kind of information making the daily news, and many consumers suffering as a consequence, both businesses and consumers are concerned and they try to find ways of protecting themselves and their customers. One of the main concerns of consumers shopping online is identity theft. Research by Jiang, Jones and Javie [16] indicates that fears about identity theft increases the likelihood of consumers’ not making online purchases. In order to ease consumer concerns many insurance companies now offer identity theft insurance protection. According to a study conducted by Swaminathan et al.[41], consumers were more concerned about information privacy than the security of electronic exchanges. This means that consumers are more afraid that their identities will be stolen than their credit card numbers. Therefore, protecting private information and having a privacy policy displayed on web sites will ease some of consumer’s concerns.

Lack of Confidence

When people experience anxiety, grief, dejection and despair they feel uncertainty, which then prevent their tendency to take action[3]. This is especially important when people are dealing with technology. When consumers attempt to purchase products online, they have to have 1) confidence on their own computers (for example: what if there is a software embedded in my computer that reads everything I type and sends it to hackers?), 2) confidence on their internet service providers (ISP) (for example: what if the my ISP is retrieving the information I submit online?), and 3) confidence on e-tailers or merchants (for example: what if the merchant who receives my private information will sell it to third parties? What if the merchant uses my credit or debit card number to make purchases online? Will the merchant deliver my order on a timely manner?). When a web site does not look professional, consumers feel uncomfortable making online purchases. The look, web site navigation, and web content are major contributors to online trust. A study showed that adding support pages to web sites can improve online trust [12].

Possibility of Shopping on Bogus Web Sites

Individuals can develop professional looking web sites in an attempt to sell merchandise that they do not have and obtain peoples’ credit or debit card information. Shady individuals also fool people into using a bogus website that resembles the authentic site of their bank or of their favorite store ("phishing") [37]. Often times, the request to go to bogus web sites come through e-mails and they look legitimate, but redirect people to bogus web sites. Just in 2004, phishing schemes accounted for approximately $2.4 billion in fraud - or about $1,200 per victim [34].

What Can Online Retailers Can Do to Build and Improve Trust with Current and Potential Customers?

Protect Private Customer information

One of the keys to keeping customer’s data private is to limit the amount of customer data that an e-tailer stores. Only data pertaining to competitive advantage should be kept. As early as 1999, security professionals have been warning e-tailers about the dangers of storing customer credit card numbers. Few e-tailers have heard the message and continue to store sensitive information for customer convenience. In an analysis performed on Amazon.com by
Ross Anderson, a lead security expert of Cambridge University [2], Anderson pointed out that e-tailer retention of credit card numbers poses a greater risk (Kabay 2003) than hackers capturing the data in transit. In 2003 a fourteen-year-old high school boy, Alberto Gonzalez, proved him right. Gonzalez working with a team of hackers and successfully gained access to approximately 180 million credit card numbers from databases from well known company’s databases including OfficeMax, Target, T.J. Maxx and Marshalls [46]. Gonzalez broke into the databases by taking advantage of a weakness discovered using software query language (SQL) now termed SQL Injection. By sending a specially designed SQL query, the hacker tricks the database into executing unintended commands and therefore bypassing proper authentication [4].

Using the SQL injection method, many hackers have bypassed database security and have stolen millions of credit card numbers. One of the latest cases concerns twenty-six-year-old Rogelio Hackett Jr. from the country of Georgia who pled guilty to breaking into an unidentified ticketing services provider’s database and stole 359,661 pieces of credit card data[38]. Since the exploitability is simple to execute and the data loss can be catastrophic, the Open Web Application Security Project Foundation (OWASP), a non-profit security awareness organization, has listed injection type flaws as the number one security risk [35].

Unfortunately, it can never be proven that a database is completely 100% secure. Therefore the best course of action for e-tailers is to not store sensitive data in the first place. Wharton marketing professors Eric Bradlow and Peter Fader recommend that companies keep only the raw data needed for competitive advantage and purge the rest. In an article written for Forbes magazine, Bradlow and Fader describe a method with which it is possible to collect and aggregate consumer information needed for competitive study while deleting the original data. This method allows e-tailers to still learn from their customers while eliminating much of the risk [23].

Needles to say, keeping customers’ private information private is crucial in building and maintaining trust with customers. Web sites need to assure consumers that their information will be kept confidential. To this end, web sites need to disclose privacy policies on their web sites and allow customers to choose how sellers can use their information. Most web sites have adopted such a policy, but this does not mean that they can keep customer information safely. This is why companies marketing their products online need use secure information technology and other measures to protect customer information. For detailed information about consumer privacy, please see the following web link: http://www.gpo.gov/fdsys/pkg/PLAW-106publ102/content-detail.html

Display Security Certificate Seal or Logo Provided by Internet Security Agencies

Studies indicate that displaying web site certification and having third-party logos on a web site can reassure potential customers and increase the probability of purchase [16]; [21]. Some examples of web site certification logos commonly seen on web sites are eCert, eTRUST, TRUSTe, and Verisign.

Having Professional Looking and Easy to Navigate Web Sites
Consumers feel confident in shopping on websites that look and feel professional. These include the ease of navigation, text, color, website page background, pictures, company information, ease of contact via email and other methods, customer support page, contact page including a mailing address, email and a telephone number, and presence of secure shopping carts. Consumers and buyers for organizations are uneasy to shop in a website that looks as if it were developed in a garage and expect certain website standards.

**One Click Purchasing Process**

Many customers abandon a site if they are asked to provide personal information each time they try to purchase something [21]. Current technology allows websites to create and retain customer profile information. Providing a one click purchasing process eliminates the time consumer’s waste in supplying information at each purchase (see for example, Amazon.com and Apple.com).

**Customer testimonials**

Kim and Kim [22] recommend that the vendors need to provide other customer testimonials and company information such as history, physical location, sales volume, number of customers and others. To maintain a trustful relationship, an online store needs to follow through on its promises at all times. In addition, many websites now provide customer reviews of their purchases. These reviews are important information about not just product quality, but also about how a company practices its business [20]. Having both positive and negative reviews is a sign of honesty. Indeed, customers view websites that display customer reviews as safe since other customers have already successfully shopped in the web site of interest. Reviews that go back in years also assure customers not only on security of the website, but also build trust.

**Monitor Employees**

Human behavior may account for a large majority of security breaches, even when all of the proper technology is in place. In 2008, a thumb drive infected with malicious code was inserted into a military laptop on a secure base [31]. In 2010, an Apple employee left an Apple iPhone prototype in a bar [32]. When management attempts to roll out security changes to combat security issues, employees often have negative reactions that result in conflict, mistrust or even paranoia. It is recommended that e-tailers identify internal as well as external risk areas. It is evident that in order to prevent security risks of employee origin, e-tailers must define, create and implement a comprehensive security plan procedures to be followed.

**Using Information Technology in Making Web Sites to Project a Secure Shopping Environment**

**Using a Secure Transaction Mechanism (SSL) via HTTPS**

Customers can verify that their data is encrypted and being transmitted over a secure channel by verifying that the HTTPS protocol is listed in the browser’s URL window (https://).

This protocol is a combination of two layered protocols. First, the Secure Sockets Layer (SSL) protocol creates an
encrypted channel for private data to be exchanged safely and securely between the shopper’s web browser and the e-tailer’s web server. Next, the Hypertext Transfer Protocol (HTTP) is the application protocol that handles the actual message traffic between the browser and the server. Security conscience e-tailers often advise their customers to shop at sites that are completely protected by HTTPS. Websites that use a mix of HTTP and HTTPS protocols are open to various hacking techniques.

**Firewalls Id Management and Intrusion Detection**

While the customers trust in e-tailers is important, the network used by e-tailers needs to have some level of trust in the data that is passed back and forth in order to make the sale. The e-tailer needs to maximize the security while still letting the sales happen. It is recommended that the e-tailer network needs to be comprised of one or more of the following devices: firewall, IDS (intrusion detection system) or DMZ (demilitarized zone, also referred as perimeter network).

**Firewall**

A successful firewall prevents unauthorized data from moving from the Internet to the e-tailer’s internal networks [13]There is a wide range of firewall security strategies from authenticating the legitimacy of the request to authenticating that person is he/she claims to be. An E-tailer’s firewall should stop all incoming message traffic not related to the business. Without a user authentication server, it is impossible for e-tailers to control the access to their database. For detailed information about firewalls, please see the following web link: [http://www.windowsecurity.com/whitepapers/ECommerce_Security_Technologies_Fire_Wall.html](http://www.windowsecurity.com/whitepapers/ECommerce_Security_Technologies_Fire_Wall.html)

**Intrusion Detection System**

An intrusion detection system (IDS) actually attempts to spot threats and alarm personnel of a potential security breach. A network intrusion system is not a firewall replacement. Firewalls and intrusion systems can help protect your data and both must be part of your overall security plan. To properly evaluate the requirements for their firewall and IDS, e-tailers should consider not only their needs for detection and prevention but also for performance and costs. For detailed information on intrusion detection system, please see a document published by National Institute of Standards and technology published by U.S. Department of Commerce [http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf](http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf)

**Demilitarized Zone (DMZ)**

A subnetwork where an e-tailer can put their servers that need to interface with the outside world. These servers are behind the firewall, but not part of the internal network. For example, it is a good idea for e-tailers to put the web server in the DMZ. Therefore all https traffic is allowed to the web server in the DMZ but not allowed into the internal network. In fact, the DMZ does not allow any connections from the outside network into the internal network.
Terminal Access Control Access Control System (TACACS+)

TACACS+ is an open standard protocol used to forward customer’s credentials to a centralized server for verification. Among other duties, it provides basic authentication functions for the shopping network. With millions of potential online shopping customers, it is a necessity to keep all customer data in one centralized location that can be adequately protected. Without a protocol such as TACACS+, it would be necessary to update several access servers whenever new customers are added [9].

The Costs of Information Technology Security Devices

Costs vary significantly depending on the security services needed and the size of customer base and network. For small enterprise, there are several good, easy-to-use; secure shopping cart vendors that provide out-of-the-box secure shopping for e-tailers. A larger enterprise may want to build and therefore control the company’s network. The security budget usually directly correlates’ with the size of the organization. Regardless if the vendor is large or small, there are many solutions that can be customized to fit a corporation’s budget that keep all customer data reasonably secure.

In addition to cost and benefit considerations, businesses need to be aware of Federal law that has been in place since 2002. Under the Federal Information Security Management Act of 2002 [33], the federal government requires that federal agencies implement policies to secure information. The National Institute of Standards and Technology (NIST) has developed a series of publications [6]; [14] to help implement the required policies and procedures. E-tailers would benefit their customer base by reviewing, adopting and advertising their security improvements and compliance with the appropriate government policies and standards.

Conclusions

When customers experience problems with online shopping they shy away and go back to their traditional purchasing behavior; shopping at brick and mortar stores or only shop at web sites where they feel comfortable. Consequences of not assuring customers of trustworthy shopping environments can be disastrous and even lead businesses into bankruptcy. Benefits of having a secure web site certainly outweigh the costs. In this paper we attempted to show how businesses could build trust and have secure web sites by culminating previous research.

To summarize our findings we provide the following suggestions for businesses. It is important to note that the following actions and strategies are not exhaustive and based on previous research:

1) have professionally developed web sites;
2) ease of navigation – customers’ being able to move from one page to another and the hyperlinks that work;
3) use appropriate web site background, pictures, and text;
4) Allowing customers to contact businesses via multiple channels such as e-mail, chat, telephone, or snail mail. This is especially true for web sites that are not well known;
5) respond to customer complaints immediately and cordially and regain unsatisfied customers by resolving issues and even offering free products or coupons towards their next purchase;
6) do not store customers’ private information unless they agree to do so – note that unless a business has very secure web sites, the private information including credit cards should not be stored at all;
7) Allow option for customers to purchase products online without registering;
8) Allow customers to purchase using a variety of credit cards and let them know that their transactions are done on a secure environment while they are at check out – this is commonly done when web sites use secure URL’s https versus http;
9) Allow customers to rate their shopping experiences on your web site including product quality, delivery, and customers service;
10) Give choice to customers not to receive promotional e-mails or newsletters;
11) have one or more of the security measures discussed in this paper such as firewall, IDS, DMZ or other, and
12) display security certificate seal or logo provided by Internet security agencies – many web sites now display padlock at a check out page.

References


