Available online at www.ijrp.org

International Journal of Research Publications

Assessment of factors that affect users' level of trust and sense of security in E-Commerce applications

Zachariah Onteri Mitaki[1], Collins Oduor Ondiek[2]

Zachariah Onteri Mitaki PhD in Business Information Systems Student from School of Informatics and innovative Systems, Jaramogi Oginga Odinga University of Science and Technology, Bondo, Kenya
Dr. Collins Oduor Ondiek Lecturer School of Informatics and innovative Systems, Jaramogi Oginga Odinga University of Science and Technology, Bondo, Kenya
E-mail: onteric@gmail.com[1], ondiekcollins@gmail.com[2]

Abstract

Electronic commerce plays a major role in any society's socio-economic progress, and now forms a fundamental part of the way people and organizations purchase products, services and conduct business. Still, its full potential still remains unfulfilled. The realisation of its potential in in Kenya will only be achieved once existing challenges, such as lack of trust and security, are eliminated. This paper had two objectives: to assess the factors that affect users' level of trust and sense of security in E-Commerce applications; To establish the relationship between trust and security in E-Commerce applications. The researcher applied mixed methods research; and data collection was done by using a questionnaire, followed by focus group discussion. The results point to the existence of an intricate relationship between user's level of trust and sense of security. Further, it was deduced that lack of security affects trust levels which leads to reduced online transactions. There is need for e-commerce organizations to ensure that adequate security measures are employed in order to gain a larger market and to increase profitability.

Key words: E-Commerce, trust, security, E-Commerce security, online transactions

1.0 Introduction

Electronic commerce is increasingly becoming part and parcel of most business setups today. There are those organisations that have fully embraced the idea of running fully pure play businesses and those that have a mix of both the online and offline operations, that is, brick and mortar. The Internet has revolutionised the world of business and commerce by creating not only great opportunities but also threats for consumers, organizations and other stakeholders. The users' perception of trust and sense of security is becoming of great concern given the Internet's openness and ubiquity making the world highly interconnected and networks such as the Internet more prone to security attacks.

Electronic Commerce is regarded as the buying and selling of products or services over the Internet, (Turban, Viehland, & Lee, 2008). Various inventions have contributed to the proliferation of Electronic Commerce. The invention of the Internet in 1969, facilitated the interconnection computer networks beyond geographical boundaries; the Electronic Funds Transfer (EFT) in 1970s, made it possible for the electronic transfer of funds from one financial institution to another; the Electronic Data Interchange (EDI) in the 1980s, facilitated the transfer of day to day business documents, thus expanding electronic transfers from only financial transactions to include other types of transaction processing; and the World Wide Web (WWW) in the 1990s; has facilitated the development of many innovative applications, ranging from online sales to e-learning experiences and other E-Commerce applications, (Turban, Viehland, & Lee, 2008).

The global digital community consists of 4.087 billion active Internet users as of April 2018, and this number continues to grow exponentially as a more increasingly digital-literate generation continues to come of age and as computing devices that deliver greater computing power are being delivered to the market at more affordable costs (Statistica, 2018). Researchers agree that all Internet users are potential customers to e-commerce companies, (Ho & Wu, 1999).

1.1 Trust in Electronic Commerce Transactions

Customers' trust as they transact through the Internet and other computer networks is important for the success and development of e-commerce. The customers' level of trust may vary from one online channel to another.

(Turban, Viehland, & Lee, 2008) define trust as the psychological status of relying on another party to achieve a particular goal. When such trust exists among the transacting parties, the confidence that each party will keeping their end of the bargain is strengthened. It is imperative that trust in E-Commerce be increased for successful online commercial transactions, (Szulanski, Cappetta, & Jensen, 2004). Actually it is now widely accepted that the Internet's currency is trust, the absence of which productive online transactions especially are impossible. It is further argued by scholars that trust can be increased by either establishing affiliations with objective third parties or by ensuring that these three key elements are present in such online engagements: integrity, competency, and security, (Szulanski, Cappetta, & Jensen, 2004).

Evidence from many researchers suggests that users' level of trust when making transactions through electronic means in the online interconnected environment is very important (Chellappa, 2008). Trust is a prerequisite for any meaningful engagements to take place, especially in online platforms where the participating parties have no face to face interactions. Thus, switching from physical to online stores may be difficult because of the perceived difficult in establishing trust (Turban, Viehland, & Lee, 2008). Building consumers' trust of e-commerce offerings is not very easy, (Someswar, Sam, & Sridhar, 2002), yet for any e-commerce undertaking to succeed it is imperative that the business must strive to build trust.

(Blaze, Feigenbaum, & Lacy, 1996) agree that dealing with issues of trust and managing trust in electronic commerce is a very difficult endeavour, which nevertheless, has to be managed through various mechanisms such as digital certificates, (Grandison & Sloman, 2000).

1.2 Security in Electronic Commerce Transactions

E-Commerce security is defined as the principles that guide safe electronic transactions, facilitating the buying and selling of goods and services through the Internet, with the use of protocols to provide safety for the parties involved, (Cardinal Commerece, 2018). Successful e-commerce depends on the customers' trust that a company has the requisite security requirements in place, (Cardinal Commerece, 2018).

The consumers' concerns about the security of online transactions forms is the biggest issue in e-commerce implementations, (Labuschagnce & Eloff, 2002); (Katsikas, Lopez, & Pernul, 2005). The research community is in agreement that the challenge of security is multifaceted, it takes both technical and nontechnical perspectives which involve the issues of organizational capacity, managerial initiatives and human dimensions, (Turban, Viehland, & Lee, 2008); (Solms, 2001). This makes it imperative that organizations that intend to trade online should take initiatives to understand the customers' security perspective and view. This is so because no matter what security technology they use, the underlying sense and perceptions of security by the customers will ultimately determine if they will trust an e-commerce website enough to trade in it.

Researchers have found that customers' perception and sense of security in online e-commerce channels affect their trust when they intend to undertake transactions (Cheskin Research, 1999); (Cheskin Research, 2000). Electronic Commerce has the potential of transforming the way consumers purchase goods and services but to a great extent, this potentiality has not been achieved, partially because of the risks associated with online trading. Consumers find it difficult to trust faceless parties on the other side of the network with sensitive personal information especially credit card transactions, (Cheskin Research, 1999).

After review of the relevant literature, the research design and methodology is presented followed by the research findings and data analysis. The discussion and recommendations section finally presented.

1.3 Problem of Research

Out of choice or necessity, the global population is increasingly adopting online transactions. The Internet-the world's largest interconnection of computer networks- has created tremendous opportunities as well as threats for participants, both the business enterprises and the consumers. Business organizations and consumers have found the use of the Internet to be a highly rewarding endeavour that has great potential in helping offer or access services online, seamlessly and with a lot of ease. This means that there will be a great deal of savings in terms of cost and time. On the other hand, the challenges of security and trust in an online environment are increasingly affecting e-commerce, thus making consumers to shy away from transacting online.

As the global frenzy of the adoption of online trading continues, the risks associated with such transactions abound. Online users may find it difficult to give sensitive personal information such as credit card information online. It is in this context that this paper seeks to assess the factors that affect users' level of trust and sense of security in E-Commerce applications.

1.4 Objectives of the study

- To assess the factors that affect users' level of trust and sense of security in E-Commerce applications.
- To establish the relationship between trust and security in E-Commerce applications.

1.5 Research Question

- What are the factors that affect users' level of trust and sense of security in E-Commerce applications?
- Is there a relationship between trust and security in E-Commerce applications?

1.6 Scope of the study

The present study seeks to assess the factors that affect users' level of trust and sense of security in E-Commerce applications in Kisii town, Kisii County, Kenya. This research was conducted on the residents of Kisii town, Kenya, aged between 18- 50 years. Only those who have made transactions online were included.

2.0 Literature Review

The literature review seeks to examine existing research on users' trust and sense of security in e-commerce applications.

(Dong-Her, Hsiu-Sen, Chun-Yuan, & Lin, 2004) opine that the perception of lack of security by online customers represents a major risk and the main impediment to the growth and development of e-commerce. (Flavia´n & Guinalý´, 2006) further demonstrate that trust in the online transactions affects the consumers' perception of security. E-Commerce sites may therefore boost customers' trust by decreasing perceived risk and improving website security, (Warrington, Abgrab, & Caldwell, 2000); (Lee & Lin, 2005) concluded that trust will encourage online transactions and will also affect customer attitudes towards e-tailers.

(McKnight, Choudhury, & Kacmar, 2002) in their research found that the quality of the information about a product or service in an e-commerce website determines the customer's level of trust. Trust is defined as the psychological state of depending on a party regarding the execution of a task, or transaction, (Turban, Viehland, & Lee, 2008). So if the quality of the content found in a website is not appealing to the user, then customer trust and satisfaction will be affected, (Park & Kim, 2003).

Researchers agree that the ease with which one can initiate and conclude online transactions is a statement on the level of security of the e-commerce website, (Davis, 1989); (Morris & Turner, 2001), and (Venkatesh & Davis, 2000). Especially, those consumers who are new to technology associate the ease of interacting with technology to be a reflection of strong security, (Gefen, 2000).

(Turner, Zavod, & Yurcik, 2001) found that the implementation of e-commerce websites is a pointer to the state of the security of the site. Weak and poor implementation of the design of such sites can be characterised

by issues such as prolonged page download duration and timeouts of web pages. However, the researchers agree that users' sense of security was dependent on the context. For instance, critical personal information such as the credit card details, require robust security; and browsing a website to look for information needed less security, (Wolf & Pfitzmann, 2000)..

The requirement to log on to a website via the log on page indicated was found to be a good security pointer since it implies that site access is only for the authenticated entity. Users associate good standards and practices for setting strong passwords with strong security. Most users confessed that they do not religiously follow the website password standards and practices especially when they access the Internet from the comfort of their homes. On such instances, a section of users prefer to use short and easy to recall passwords. The users even use the same password for more than one sites, mainly because of the fear that they may forget the passwords, (McCauley-Bell & Crumpton, 1998); (Cheskin Research, 2000).

(Turner, Zavod, & Yurcik, 2001) found out that brand recognition of e-commerce sites by the online users is an important pointer the level of security. Thus, a good reputation and satisfactory customer service of the online company means strong security. The opposite was also found to be true. The online company's reputation and customers' experience in such sites affected the consumers' level of trust and sense of security as pertains to the ability of the site to protect their data. The policies and practices of e-commerce companies were found to be a statement on security of transactions, which also affects the users' level of trust.

(Turner, Zavod, & Yurcik, 2001) further argue that responsiveness in online transactions affect both the level of trust and sense of security of consumers. This view is also supported by (Gefen, 2000). Responsiveness is a pointer to an organization's willingness and ability and to promptly attend to queries raised by the customers, (Zeithaml, Parasuraman, & Malhotra, 2002). Online companies should provide a mix of channels like online

chat, e-mail and phone contacts for the diverse groups of customers in order to provide an avenue for queries and responses, (Turner, Zavod, & Yurcik, 2001).

Another key factor that was found to contribute to the level of trust and sense of security online is the aspect of endorsement from third parties. This may be recommendations from relatives and friends, affiliations of online companies to highly reputable independent organizations. Users felt an assurance of security against fraud and a sense of credibility in the presence of such endorsements. (Turner, Zavod, & Yurcik, 2001).

3.0 Research Design and methodology

3.1 Introduction

This section focusses on: research design, target population, sample size and sampling procedure, research instruments, validity of the instruments, reliability of the instruments, data collection procedures.

3.2 Research design

A research design is the arrangement of conditions for collection and analysis of data in a manner that aims to combine relevance to the research purpose with economy in procedure (Kothari, 2004). This study adopted quantitative and qualitative research design (mixed methods research).

3.3 Target population

This study targeted the residents of Kisii town, Kenya.

3.4 Sample size and Sampling procedure.

According to (Kothari, 2004), sample size is a sub population that you are taking from the target population in order to carry out your study. Purposive sampling was employed by including only those respondents who have participated in the buying and selling of goods and services through the Internet. Based on the purposive sampling design, a total of 100 respondents were involved in the study.

3.5 Research instruments

The data collection instruments included questionnaires and focus group discussions. By structure, the questionnaire required a mix of close ended and open ended responses so has to help the researcher achieve his interests of mixed methods research.

3.6 Validity of the instruments

Validity of the instruments used is a pointer to the accuracy of the collected data. It is the extent to which differences found with a measuring instrument reflect true differences among those being tested, (Kothari, 2004). To achieve this purpose, the questionnaire was piloted in order to validate the research instrument being used based on three criteria: Content validity; Criterion-related validity; and Construct validity. The piloting was done by giving the questionnaire to ten respondents. Necessary corrections were then made to the questionnaire.

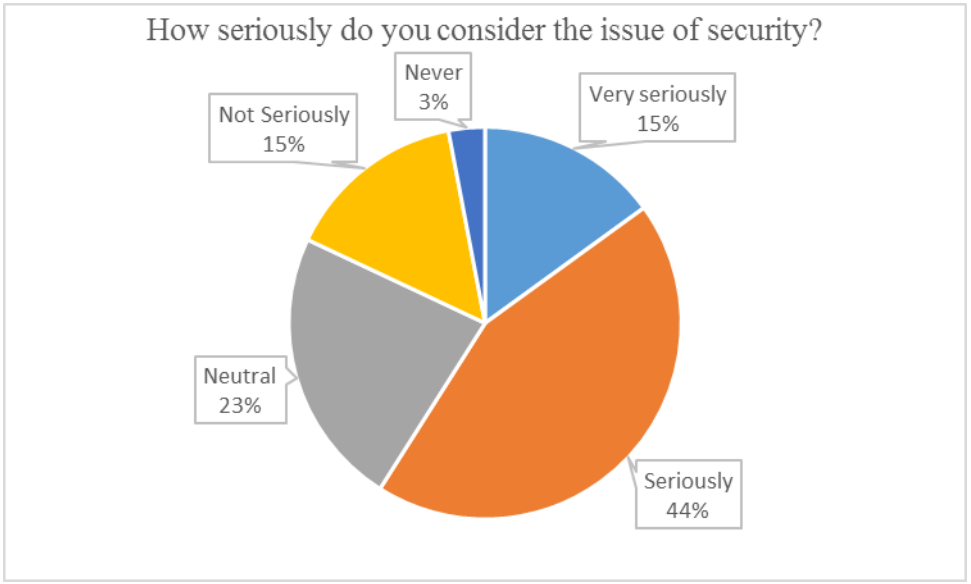
3.7 Reliability of the instruments

According to (Best & Khan, 2006), if a co-efficient of 0.5 or more is attained, then the study instruments would be adopted for use. In this study, a correlation coefficient was obtained and it indicated the reliability of the instrument used. Pearson's product moment correlation co-efficient was used to correlate the scores and this was taken as an estimate of reliability.

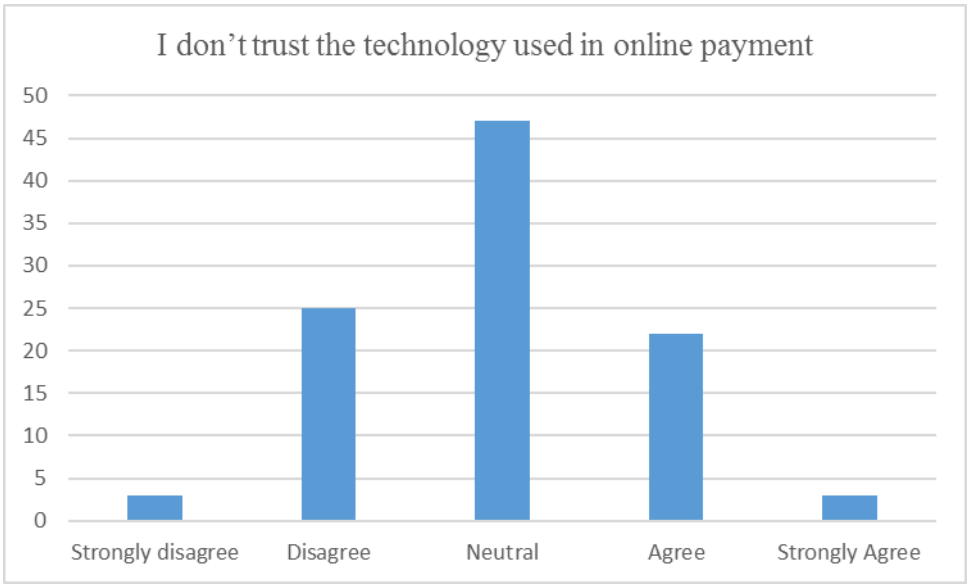
4.0 Research findings and analysis

One hundred respondents aged between 18-50 years participated in this study. After the responses from the participants were received, the researcher put together and examined the correctness of the responses. This was then followed by a focus group discussion between the researcher and all the 100 respondents. All the responses were analysed and contentious issues were discussed in order to achieve a middle ground. The participants' responses regarding their level of trust and sense of security were analysed.

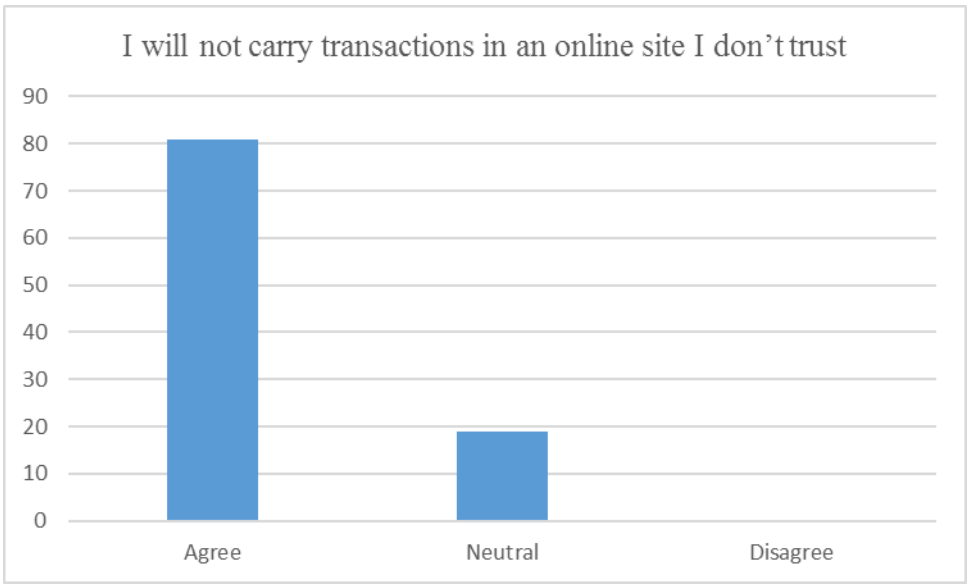
44 % of the respondents consider the issue of security seriously, 23% were unsure about the security requirements and considerations, 15 % very seriously, 15% not seriously, and 3 % never consider the security issues when making transactions.



When responding on the level of trust to the technology in online payments, 47% were neutral, 25% do not trust the technology, 28 % trust the online payment technology.



81% of the respondents will not carry transactions in an online site they don't trust, 19 % were neutral.



88% of the respondents won't feel secure sending sensitive information over the internet, 12% don't care. 90% will use online services if the security technology is improved as opposed to 10% who will not use the online services even in such circumstances. 89 % of the respondents feel that actions such as new laws, two-

factor authentication, biometric security, and security programs can improve online security, 51% believe that e-commerce sites are committed to ensuring online security, 87% will not purchase from an online site they do not trust. 86% agree that the level of trust they have towards a site will influence their decision on the site to purchase from; and 88% agree that third party referrals will influence their trust and security perceptions. 89% agree that factors such as ease of use, responsiveness, quality of the information, implementation, log on page, brand recognition and redress against are an indication of strong security.

Question	**Agree**	**Disagree**
I wouldn't feel secure sending sensitive information over the internet	88%	12%
I will use online services if the security technology is enhanced	90%	10%
Actions such as new laws, two-factor authentication, biometric security, and security programs can improve online security	89%	11%
I trust that e-commerce sites are committed to ensuring online security	51%	49%
I will purchase from an online site I do not trust	13%	87%
The level of trust I have towards a site will influence my decision on the site to purchase from	86%	14%
Third party referrals (such as relatives, friends, family and other independent online parties) influence trust and security perceptions	88%	12%
Factors such as ease of use, responsiveness, quality of the information, implementation, log on page, brand recognition and redress against fraud are an indication of security	89%	11%

5.0 Discussion

It came out clearly that the users' level of trust and sense of security are intricately tied together. The opposite holds true. When the trust levels are low, the users can not feel secure transacting in such a site; again, when the e-commerce website does not possess the requisite security features, the users show disdain for such a site because of the absence of trust.

The user's level of trust and sense of security have an impact on the willingness of the consumers to carry out transactions on a website. Most of the users were quick to point out that the ease with which one can initiate and conclude a transaction is a pointer to the level of security of a site. Those sites that give users a difficult time in the execution of their transactions were said not to pay attention to detail, thus they were considered not to be paying attention to the security of the site. The researcher also found out that the users associated long page loading times, and web page time-outs to weak security of the site, hence this affected the trust levels and sense of security.

The researcher established that users who had knowledge of how to determine if the site in which they are transacting is secure are bound to carry out more transactions online regularly with confidence as opposed to those who do not have the knowledge on how to verify the security status of a site. Though most of the users admitted that they never check the SSL Certificate, there was greater consensus, after discussions, of the need to check the SSL certificate. A few of the team members showed knowledge of how to determine that, for instance, if the URL of the website begins with "https" it means the site is secured using an SSL Certificate. The users also concluded that the availability of the symbol of a padlock and a correct domain name also affected their view of the security of a website. The users were well aware that some rogue sites may mimic the design of genuine sites and thus the domain name was the only way to differentiate them, albeit the slight variations that may confuse those who are not keen enough.

It was established that redress against fraud was another key factor in determining the level of trust and sense of security in a site. The users look at this issue in a two dimensional perspective: first, if the services offered are unsatisfactory; or, two, if the online site in which they transacted was a fraud that was only interested in stealing from the consumers. The users were unaware of any redress mechanisms in case of fraud or unsatisfactory services in e-commerce sites. Particularly, e-commerce users are worried by two facts: the difficult of detecting online fraud; and, online fraud may sometimes be cross-border, so in such situations, which laws should be applied? Effective redress mechanisms will boost the trust and sense of security of the customers which will in turn be a boon to online business environments as more 'pane shoppers' will willingly engage in online transactions.

The quality of information found in an e-commerce website, the effectiveness of responses to customers' queries, log on page combined with strong password policy, and brand recognition and company reputation all contribute to trust and security perceptions in online applications. A lack of this will affect the user's ability and willingness to openly transact in the online platforms.

Independent third party endorsements also affect the level of trust and sense of security in an e-commerce website. Worth noting is the fact that websites recommended to a user by family members, relatives, friends or colleagues are more trusted and users feel more secure transacting in them. This emanates from the fact that the independent third parties share experiences that help inform their choices for sites in which to transact. Sites in which any of the parties may have encountered bad interactions and experiences are all given a wide berth. Users were in wider agreement that if they were referred by an advertisement banner in a trusted website, they could click on the banner, with an assurance that it led to a secure site.

5.1 Conculsion and recomendations.

As presented in the findings section above, the factors are clearly assessed and it is established that trust and security are interrelated subjects that affect each other. They are interlinked and will affect consumers' attitudes and perceptions when transacting online. Trust and security are the most important considerations by users when transacting in online environments. Any perception that a website is insecure results in trust deficit which will ultimately influence the choice of the site to transact in.

In order to capture a larger market, e-commerce sites must invest in assuring consumers of the security of their transactions. This must be done by boosting trust levels through better security mechanisms, the absence of which will lead to decreased number of customers for the online sites.

6.0 References

Best, J. W., & Khan, J. V. (2006). Research Methodology, Fifth Edition. New Delhi: Prentice Hall.

Blaze, M., Feigenbaum, J., & Lacy, J. (1996). Decentralized Trust Management. IEEE Symposium on Security and Privacy, (pp. 164-173).

Cardinal Commerece. (2018). Cardinal Commerce. Retrieved from Cardinal Commerce Website: https://www.cardinalcommerce.com

Chellappa, R. K. (2008). Consumers' Trust in Electronic Commerce Transactions: The Role of Perceived Privacy and Perceived Security. Under Submission, 1-38.

Cheskin Research. (1999). E-Commerce trust study.

Cheskin Research. (2000, July). Trust in the wired Americas. Retrieved from www.cheskin.com: http://www.cheskin.com/think/studies/trust2.html,

Davis, F. (1989). Perceived usefulness, perceived ease-of-use, and user acceptance of information technologies. MIS Quarterly, 319-340.

Dong-Her, S., Hsiu-Sen, C., Chun-Yuan, C., & Lin, B. (2004). Internet Security: Malicious E-mails Detection and Protection. Industrial Management & Data Systems, 613-623.

Flavia´n, C., & Guinalý´, M. (2006). Consumer Trust, Perceived Security and Privacy Policy: Three Basic Elements of Loyalty to a Web site. Industrial Management & Data Systems, 601-620.

Gefen, D. (2000). E-commerce: The role of farmiliarity and trust. International Journal of Management Science, 725-737.

Grandison, T., & Sloman, M. (2000). A Survey of Trust in Internet Applications. IEEE Communications Surveys and Tutorials.

Ho, C., & Wu, W. (1999). Antecedents of Customer Satisfaction on the Internet: An empirical study of online shopping . Hawaii International Conference on Systems Sciences, (pp. 1-9). Hawaii.

Katsikas, S. K., Lopez, J., & Pernul, G. (2005). Trust, Privacy and Security in e-business: requirements and solutions. 10th Panhellenic Conference on Informatics, (pp. 548-558). Volos, Greece.

Kothari, C. R. (2004). Research Methodology: Methods and Techniques; Second Revised Edition. Jaipur: New Age International (P) Ltd.

Labuschagnce, L., & Eloff, J. (2002). Electronic commerce: the information security challenge. Information Management & Computer Security, 154-157.

Lee, G., & Lin, H. (2005). Customer Perceptions of E-service Quality in Online Shopping. International Journal of Retail and Distribution Management, 161-176.

McCauley-Bell, P., & Crumpton, L. (1998). The human factors issues in information security: what are they and do they matter? Human Factors and Ergonomics Society 42nd Annual Meeting, (pp. 439-443). Chicago.

McKnight, D., Choudhury, V., & Kacmar, C. (2002). Developing and Validating Trust Measures for E-commerce: An Integrative Typology. Information Systems Research, 334-359.

Morris, M. G., & Turner, J. M. (2001). Assessing users' subjective quality of experience with the World Wide Web: an exploratory examination of temporal changes in technology acceptance. International Journal of Human-Computer Studies, 877-901.

Park, C., & Kim, Y. (2003). Identifying Key Factors Affecting Consumer Purchase Behavior in an Online Shopping Context. International Journal of Retail & Distribution Management, 16-19.

Solms, B. V. (2001). Information security–A multidimensional Discipline. Computers & Security, 504-508.

Someswar, K., Sam, R., & Sridhar, N. (2002). A framework for analyzing e-commerce security. Information Management & Computer Security , 149-158.

Statistica. (2018, May 15). Statistica. Retrieved from www.statistica.com: https://www.statista.com/

Szulanski, G., Cappetta, R., & Jensen, R. J. (2004). When and How Trustworthiness Matters: Knowledge Transfer and the Moderating Effect of Casual Ambiguity. Journal Storage (JSTOR), 600-613.

Turban, E. D., Viehland, D., & Lee, J. (2008). Electronic Commerce- Managerial Perspective. Pearson International Edition.

Turner, C. W., Zavod, M., & Yurcik, W. (2001). Factors that Affect the Perception of Security and Privacy of E-Commerce Web Sites. Fourth International Conference on Electronic Commerce Research, (pp. 1-9). Dallas.

Venkatesh, V., & Davis, F. D. (2000). Atheoretical extension of the technology acceptance model: four longitudinal field studies. Management Science. 186-204.

Warrington, T., Abgrab, N., & Caldwell, H. (2000). Building trust to develop competitive advantage in e-business relationships. Competitiveness Review, 160-168.

Wikipedia. (2017). Kisii, Kenya. Retrieved from Wikipedia: https://en.wikipedia.org/wiki/Kisii,_Kenya

Wolf, G., & Pfitzmann, A. (2000). Properties of protection goals and their integration into a user interface. Computer Networks, 685-699.

Zeithaml, V., Parasuraman, A., & Malhotra, A. (2002). Service quality delivery through web sites: A critical review of extant knowledge. Journal of the Academy of Marketing Science, 362-375.