University of Salford MANCHESTER

Salford Business School

ISSUES IN ELECTRONIC COMMERCE & HOW THEY ALTER CONSUMERS' CHOICE OF ONLINE PAYMENT

Dogus Aygun

Student ID: @00379863

A dissertation is submitted in partial fulfilment of the requirements of The University of Salford for the degree of MSc Information Systems Management

November 2014

Salford Business School

Declaration on Conduct of Assessed Work

(Academic Good Conduct)

Assessed work which does not have this form attached will be returned unmarked.

Programme & Year: MSc Information Systems Management, 2013 November Intake

Module: Business Innovation Project: Dissertation

Module Tutor: Alex Fenton

Tutorial Group: ______

Assignment Title: Issues in Electronic Commerce & How They Alter Consumers' Choice of Online Payment

Briefly, unfair means in assessed work is likely to fall into one or more of the following categories:

- Plagiarism.

Plagiarism involves taking the work of another person or source and using it as if it were one's own. Work includes, but is not restricted to, written work, ideas, musical compositions, computer programs, laboratory or survey results, diagrams, graphs, drawings and designs.

- Collusion.

Collusion involves working with others on tasks that should be carried out on an individual basis. Collusion should not be confused with collaborative work which is sometimes used as a means of learning. It will be clearly stated when collaborative work is permitted in an assessment. Unless advised otherwise, any work which is submitted for assessment must be produced by individual students.

- Falsifying experimental or other investigative results.

This could involve a range of things that make it appear that information has been collected by scientific investigation, the compilation of questionnaire results, etc. whereas in reality it has been made up or altered to provide a more favourable result.

- Contracting another to write a piece of assessed work.

This involves any means whereby a person does work on behalf of another. It includes assessments done for someone else in full or in part by a fellow student, a friend or family member. It includes sitting an examination for someone else. It also covers obtaining material from Internet 'cheat sites' or other sources of work. Penalties for this type of unfair means are likely to apply both to a student who does work on behalf of another and one who has work done for him/her.

I declare that

- **this work is my own**
- **if this is a group project, each student has contributed to the work in accordance with the set criteria**
- **the work of others used in its completion has been duly acknowledged**
- **experimental or other investigative results have not been falsified**
- **I have read and understood the University Policy on the Conduct of Assessed Work (Academic Good Conduct)***

***http://www.academic.salford.ac.uk/aqa/sections/28_conduct_assessed_work.pdf**

It is the student's responsibility to be aware of this policy and procedure.

Signature ______

Name (print): Dogus Aygun

ID Number: @00379863 Date: 10/11/2014

ABSTRACT

There has been an on-going rapid rise in Internet connectivity and expansion of internet. Developments in E-Commerce and the internet resulted in a big boom of online shopping. Consumers can now easily find and buy products online. Along with these, scams frauds and information theft are also growing and many internet users get affected by those. Unfortunately, depending on some factors which are stated in this study, security and privacy issues affect consumers' perspective about shopping and the selection of online payment method. This study addresses those issues by using a qualitative research method.

ACKNOWLEDGEMENT

I would like to thank my supervisor *Alex Fenton* for his generous guidance and for his support for giving me the right advice at the right time.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

List of Abbreviations

UK: United Kingdom

TR: Turkey

EU: European Union

PKI: Public Key Infrastructure

SSL: Secure Sockets Layer

1.0 INTRODUCTION

1.1 Background

E-Commerce is growing every day. Because of this growth of electronic commerce, transferring money online has become an important issue to consumers. (Ozkan, Bindusara and Hackney, 2010). Online electronic payment (E-Payment) plays a significant role when it comes to e-business and e-commerce. According to He et al., (2008) online e-payment is becoming more and more important each passing day. However, the *“growth of e-commerce has made the internet an enticing playground for hackers and crackers”* (Singh and Waddell, 2004*). Internet has become a dangerous place and* things like electronic shopping, electronic banking and of course the “electronic payment” requires internet connection to work. *(Teoh et al., 2013).*

There are many problems that are being encountered by both customers and e-merchants about online payment. In general, internet users are often worried about sending sensitive data through the internet. Since consumers who shop online are also internet users, they are reluctant to send sensitive information to shopping sites since those data might be stolen by hackers. Especially, if that sensitive data include credit card information or any other information about an e-payment tool, consumers worry more. Pavlau (2001, cited in Chatal, Sahi & Rani 2014, p. 2) say that because of the risk concerns, customers show unwillingness to make their payments through credit cards. Karimov et al. (2011) claims that it has been empirically confirmed that cybercrime theft and fraud negatively affect consumers who shop online.

According to Ozkan, Bindusara and Hackney (2010) *“One of the major concerns with regard to e-payments is noted to be security.”* They add that; *“the reason for that is because money and information are exchanged online without any direct engagement with the recipients”. “Security has become one of the most important issues that must be resolved first to ensure success of e-Commerce” (Hasan and Sobhan, 2012).*

According to Laudon & Traver (2013) there are two different approaches to E-Commerce: Behavioural and Technical. The reason of that is because electronic commerce is a huge & multi-disciplinary area (Khosrowpour, 2009). According to Laudon & Traver (2013) E-Commerce involves three broad inter-related themes: These are: *Technology, Business and Society. In addition to those* Nesbit (2001) identifies *society* as *“Social Science.”*

Laudon & Traver (2013) say that there are people who are interested in development of computer software & hardware and these people are mostly Computer Scientists which they are primarily focused on ‘’application of internet technology’’ In addition to ‘’computer scientists’’, there are ‘’management scientists’’ which they are interested in building technical business models. However, again according to Laudon & Traver (2013) behaviour area is different. Instead of focusing on issues like those, behaviour area focuses things such as digital goods and pricing. Also this area includes ‘’sociological perspective’’ which includes things like social networks and communications. The challenge about electronic commerce is, in order to grasp electronic commerce entirely, variety of disciplines are needed. Which means; *''No one perspective dominates research about e-commerce'' (Laudon & Traver 2013).*

In this dissertation, the issues and how they alter consumers have been researched. Some of those issues, especially the literature review have some technical parts about the web and information systems*. Because "in order to understand e-commerce*, a basic IT understanding is needed" (Laudon & Traver, 2013).

1.2 Research Aims, Objectives and Research Rationale:

Rojon and Saunders, (2012) state that in order to build a high quality research, clear research objectives should be supported by a convincing rationale. E-Commerce is a popular research area and there are many studies being published around this area. Since payment systems and shopping choices includes both technical and sociological/behavioural part as explained above, focusing on those issues would be beneficial in order to grasp a better understanding about the e-commerce.

Aim:

- This research intends to identify and examine the important issues and concepts in e-commerce that alter the consumers' method of payment.

Objectives:

- To identify security and privacy issues in E-Commerce

- Gathering data from two different countries by using surveys and interviews in order to spot the differences & similarities about perception towards online payment.
- Gathering secondary data from variety of sources in order to support the primary data and the findings.

1.3 Outline of the Study:

Literature Review: Literature Review divided into two chapters; *security and privacy*. In first chapter, some security issues in e-commerce and dimensions of security are explained in detail. In the second chapter, the concept of privacy in e-commerce is examined.

Research Methodology: Research methodology comes after the literature review since literature section was completed before the methodology. This study adopts Interpretivism as a paradigm; questionnaires and interviews are conducted and a qualitative perspective is used.

Analysis of Results: Interviews and surveys are analysed in this section. In addition to those, some concepts are discussed by combining survey and interview results into the discussion together.

Conclusions and Recommendations: Overall conclusion and some recommendations are given based on the results and literature findings of this study.

1.4 LIMITATIONS:

Sample size is the main limitation of this study. For example; there aren't any balances between female-male and the devices they use and lack of this data prevented some analysis about certain devices. Also this study only focuses two countries which mean two different cultures. Since there are many countries in this world and their cultural values may result a totally different result. In summary: a much larger sample is needed in order to have more generalizable results.

2.0 LITERATURE REVIEW

This literature review is divided into two parts. The first part focuses on security issues and gives information about important threats and dimensions. The second part focuses on electronic commerce (e-commerce) privacy which is a major problem not just only for online shoppers but also for every internet user.

2.1 SECURITY

2.1.1 DIMENSIONS OF ELECTRONIC COMMERCE SECURITY

According to Laudon & Traver (2013) e-commerce has six dimensions regarding security. These are *Integrity, Nonrepudiation, Authenticity, Confidentiality* and finally, *Availability.*

2.1.1.1 Integrity

Integrity means that the information on a web site has not been altered by any party who do not have official permission or approval. Singh (2014) gives an example about the loss of integrity. Loss of integrity happens when the content of a message is changed after the sender sends it.

DIMENSION	CUSTOMER'S PERSPECTIVE	MERCHANT'S PERSPECTIVE
Integrity	• Has information I transmit or receive been altered?	• Has data on the site been altered without authorization? Is data being received from customers valid?

Table 1 - Integrity Source: Laudon & Traver (2013)

Data flows through networks. Rachana (2013) says that data can be altered while the data is passing to the receiver. However, when that data has a ''signature'' any change in that data will remove the signature and the data will become invalid.

2.1.1.2 Non-repudiation

Non-repudiation is there to ensure that the consumers who do online shopping do not deny that they have participated. Rouse (2008) identifies non-repudiation as '*'the assurance that someone cannot deny something*.'' However she also adds that there is no 100% fool proof security system, digital signature does not guarantee this. Normally on the internet, a digital signature is used in order to be sure that the document(s) or message(s) have been signed (electronically) by the one specific person so the person cannot make any denials about this later. Laudon & Traver (2013) adds that merchants do not obtain a physical copy of a signature and because of that, the credit card company will choose the customers side against the merchant (most of the time). E-Lock (n.a) says that this replicates the ''real world'' because when someone signs a document, that person is legally bound to the content of the document and it is the same thing about the digital signature.

DIMENSION	CUSTOMER'S PERSPECTIVE	MERCHANT'S PERSPECTIVE
Non-Repudiation	• Can a party to an action with me deny taking the action?	• Can a customer deny ordering products?

Table 2 - Non-repudiation, Source: Laudon & Traver (2013)

However according to InfoSSL (2014) a digital signature is sometimes confused with a digital certificate. *''Digital certificate is kind of a passport that allows the user to exchange information securely on the internet using the "Public Key Infrastructure (PKI)"* (Rouse, 2014).

2.1.1.2a Public Key Infrastructure

A Public Key Infrastructure enables users of a basically unsecure public network such as the internet to securely and privately exchange data and money through the use of a public and private cryptographic key pair that is obtained and shared through a trusted authority'' (Rouse, 2006). Singh and Waddell (2004) identify PKI as a technology that enables users of a network to authenticate identity and to securely and privately exchange information through the use of PKC. According to Murray (2003) ''The Public Key Cryptography needs to develop a public key infrastructure'' Certificate service providers (CSP) as known as third parties provide the Public Key Infrastructure and mostly those service providers are ISP organizations or other IT providers. Al-Slamy (2008) says that the Public Key Infrastructure creates an environment where any internet user can carry certificates that can identify them in variety of ways.

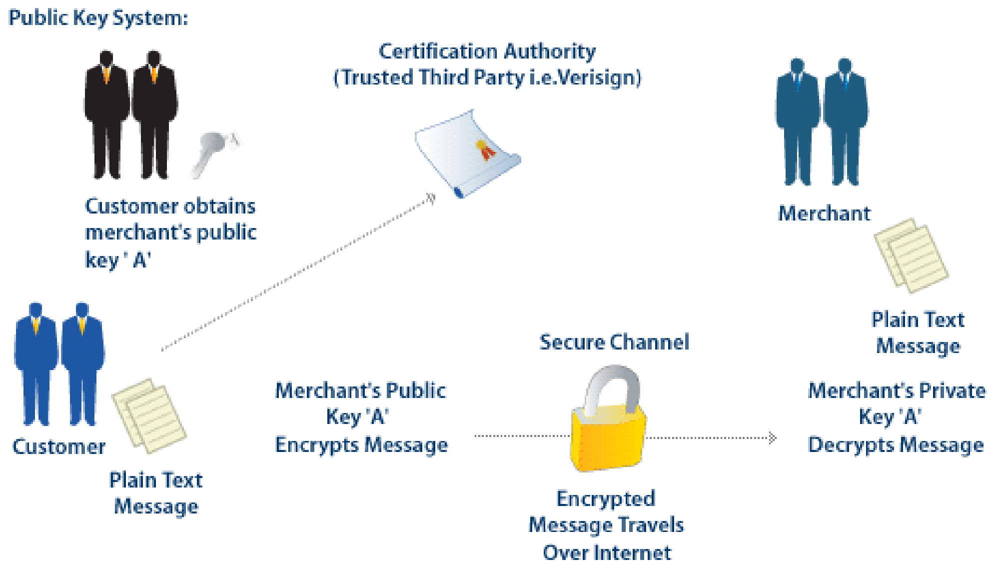

Figure 1 – Public Key System. Source: MerchantSelect (2001)

2.1.1.2b Digital Signature vs. Traditional (Handwritten) Signature

McCullagh (2000) asks the question that ''should a digital signature be treated differently from a traditional signature? According to Fillingham (1997) digital and traditional signatures have some things in common. Firstly, both digital and traditional signatures provide integrity, authentication and non-repudiation. Secondly, both have "legal standing". However there are some significant differences between digital signature and traditional signature. Perhaps the most significant difference is a witness for the signature. Traditional signatures can be witnessed but digital ones cannot be. According to Lim, (2003) authentication, integrity and non-repudiation indicate presence of trust. Traditional (handwritten) signatures are reliable because paper with watermarks, letterheads etc. makes the signature original. However on the internet those things do not exist and cannot be utilized without cryptography (Lim, 2003).

Fillingham (1997) say that mechanisms of forgery for both are fundamentally different. Forgery about handwritten signatures has been practiced for centuries; it is possible to fake a traditional signature. McCullagh (2000) adds that paper-based environment is an ‘’absolute-trusted-system’’ because there is an absolute control on the signing mechanism. However if a private signature key is absent it is impossible to fake a digital one. On the other hand since the work of Fillingham (1997) is somewhat out-dated, Entrust (2003) claims that digital signatures can be misused. Entrust (2003) also claims that digital signatures give e-business an advantage since using digital signatures instead of signing a paper and faxing it is more efficient and the processes become automated. Digital signatures increase the efficiency, lower the costs and helps the relationships.(partner, customer etc.). Brightlabs (2013) supports this and states that using e-signatures can make a business more eco-friendly and it will cut some costs and save time.

2.1.1.3 Authenticity

“Authenticity is the ability to identify the identity of a person or entity with whom you are dealing on the internet” (Laudon & Traver, 2013). According to Rouse (2007) “Authentication is the process of determining whether someone or something is, in fact, who or what it is declared to be”

DIMENSION	CUSTOMER'S PERSPECTIVE	MERCHANT'S PERSPECTIVE
Authenticity	• Who am I dealing with? • How can I be assured that the person or entity is who they claim to be?	• What is the real identity of the customer?

Table 3 – Authenticity. *Source: Laudon & Traver (2013)*

With log-on /sign-in passwords, the authenticity is guaranteed, at least it is assumed to be. However ''log on'' system have a huge flaw especially, when it comes to some specific transactions. Because when it comes to ''money transfer'' and if the amount is high, the security cannot be guaranteed (Rouse, 2007). The reason for this is passwords can be stolen easily (or even guessed). Rouse (2007) explains the reason that the online transactions have more ''strict'' process which includes digital signatures, certificates etc. as explained above. Singh and Waddell, (2004) explain that the passwords are the most common method of authentication for computer systems today. System ensures that password matches and authenticates the user. Singh and Waddell, (2004) add that login attempts should be limited and they claim that changing passwords often increases the security of an account.

2.1.1.4 Confidentiality & Privacy

Confidentiality is often confused with privacy. However they are actually two different things. "Confidentiality is the ability to assure that the data is only available to those who are authorized to view them" (*Laudon & Traver, 2013).*

Fienberg (2006) thinks that data privacy protection is one of the major problems in e- commerce. He adds that "SSL encryption" may help businesses with the protection of data since problems in privacy are many.

DIMENSION	CUSTOMER'S PERSPECTIVE	MERCHANT'S PERSPECTIVE
Confidentiality	• Can someone other than the intended recipient read my messages?	• Are messages or confidential data accessible to anyone other than those authorized to view them?
Privacy	• Can I control the use of information about myself transmitted to an e-commerce merchant?	• What use, if any can be made of personal data collected as part of an e-commerce transaction?

*Table 4: C*onfidentiality & Privacy - *Source: Laudon & Traver (2013)*

Since privacy is directly about ''control over information of people'' the confidentiality concerns about the data. A perfect example of violation of confidentiality and privacy is an incident occurred in Stanford Hospital in Palo Alto (California, USA). A privacy breach happened and about 2,000 patients' information end up on a paid-homework website as an example file how to convert data in to a bar-style graph. This data became available to everyone and it was accessible for over a year. (NewYorkTimes, 2011). Another example which is e-commerce based: A hacker hacks an e-commerce website and reaches some information and gathers customer data. If this happens the “confidentiality of the data” and the “privacy of customers” are violated. This example shows how privacy and confidentiality are actually related and why they are different concepts also.

2.1.1.5 Availability

Availability is prevention against data delays or removal. (Niranjanamurthy and Chahar, 2013). Availability is concerned with if the website and/or server is good to use when it is needed. The website is a ‘’key to success’’ for almost all organizations who are in e- commerce business. Gibson (2011) states the fact that the Information Technology Security practices focus on loss of integrity, confidentiality and availability. These three are mentioned as the ‘’security triad’’ in the literature. Availability is crucial because systems need to be up and running when they are needed. Lack of availability can and will likely do damage to e-commerce business.

Figure 2 – CIA Security Triad. Source: (ISA.co.uk)

DIMENSION	CUSTOMER'S PERSPECTIVE	MERCHANT'S PERSPECTIVE
Availability	• Can I get an access to the site?	• Is the site operational?

Table 5 - Availabilty Source: Laudon & Traver (2013)

2.1.1.5a *A Personal Anecdote about "Availability":*

Just recently, I started to play a MMO game called "Eve Online" which has a different subscription system compared to other MMO games out there. Eve Online allows players to extend their game time by buying an in-game item called "PLEX" (Pilot's License Extension). (Also it is still possible to subscribe by paying monthly instalments.) I wanted to check my subscription status from the website since I wanted to pay or buy the in-game item in order to extend my game time. However I could not access the site. At the same time all servers did not respond and the game itself did not work. I learned from social media that the website and the servers are under "DDOS" attack[1] *which is a major threat to E-Commerce security.*

[1] https://twitter.com/EVE_status/status/502550964784885761

2.2 THREATS TO E-COMMERCE SECURITY

When it comes to e-Commerce, anyone who has the technology, capability and the desire can cause harm. Threats can from inside or outside (internal & external). Both Hasan & Sobhan (2012) and Singh (2014) say that there are three vulnerable areas in electronic commerce. These are:

No #	Vulnerable Area
1	Hardware Security
2	Software Security
3	Environment Security

Table 6: Vulnerable Areas - Adapted from Hasan & Sobhan (2012) and Singh (2014)

Hardware Security is about the devices behind the e-commerce site. That hardware is needed to run the e-commerce site. Those can be database servers, network devices or even the computer or device of the client. Singh (2014) says that securing the network with a secure firewall is essential when it comes to security of network. A firewall is the main tool for the protection of Internal Systems. According to American Heritage Science Dictionary (2002), A firewall is "a software program designed to protect a network by preventing unauthorized users from gaining access or by monitoring transfers of information to and from network" According to Singh and Waddell (2004) *"a* *firewall is a network node consisting of both hardware and software that isolates a private network"*

However since firewalls inspect and scan every part of the system, (mostly) it affects the performance of entire network. Another problem with firewall is the management of it. Managing a firewall can be difficult, especially if there are many changes and exceptions going on. According to Gray (2003) good security starts at the host and a good firewall policy should be built on host based protection. A firewall which configured properly will keep out 95% of the trouble makers (Singh and Waddell, 2004). On the contrary, Gray (2003) concludes that firewalls are both '*'friend and foe''*. Laverty, (2014) explains that firewalls create considerable problems such as "the restrictions." And Laverty (2014) adds that explains that "*the firewall policies can be very restrictive and can limit users from performing legitimate operations"* However Laverty (2014) and Bocij and Chaffey (2003) examined that firewalls cannot offer protection against sabotage from inside or copying valuable data since the attacker has already have the "access" to the network.

Any software which runs the electronic commerce system (even the web browser) is a part of **software security**. Hasan & Soban (2014) claim that the main part of the security is actually the operating system. Supporting this, Yang (2003) says that Operating system has a crucial role in computer systems and security problems with an operation system will likely to cause impact(s) to the general security of the system. **Environmental security** is totally about ''physical security''. Server devices need to be protected. Singh (2014) adds that when an employee quits a job or leaves the company, all of his/her access should be removed. A search done by Software Engineering Institute (2013) shows that 23 per cent of e-crimes have been caused by insider threats. (Image)

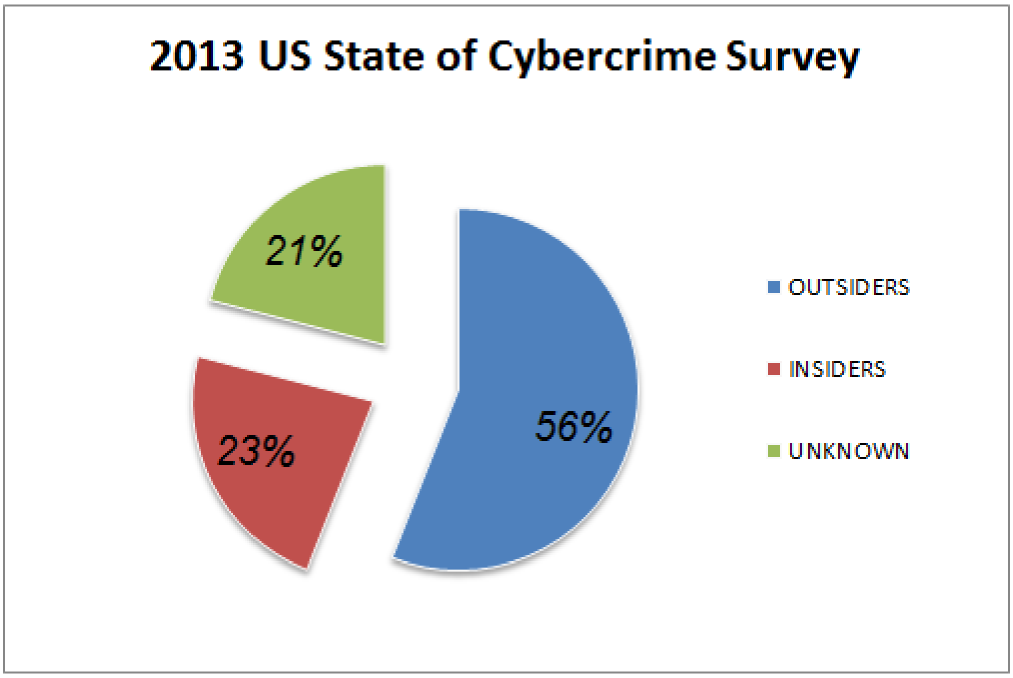

Figure 3 – 2013 US Cyber Crime Survey – Source: Software Engineering Institute CERT Program at Carnegie Mellon University (Adapted)

2.2.1 Situation of SMEs today against the security threats

There has been an increase of cyber-attacks against electronic commerce, since lots of small and medium enterprises (SMEs) go online. In the past, attacks were more concentrated on larger organizations. Because of that online organizations invest in Information Technology and Security more than SMEs since they obviously have more budgets. A. Coburn (security director in Dell) says that SMEs increasingly are being targeted, although, he adds that many claim that SMEs are not actually being targeted and they are actually under the radar against those threats (ComputerWeekly, 2011). According to Brandon (2014) SMEs are more attractive to hackers because they have a weaker online security, an example for that is SMEs doing business via cloud services that do not have strong encryption technology.

2.2.2 DDOS Attack

DDOS Attack (Distributed denial of service attack) is a malicious type of attack to a website/network. Mittal, Shrivastava and Manoria (2011) states that there are two stages of a “DDOS attack” First stage is finding “Zombies” in order to do that the hacker(s) compromise systems that are accessible by the internet. Zombie is a term for computers which are covertly taken over in order perform some actions. After this is done “zombie army” becomes available. As for the second stage, the hacker(s) use those “zombie computers” to launch an attack against the victim server.

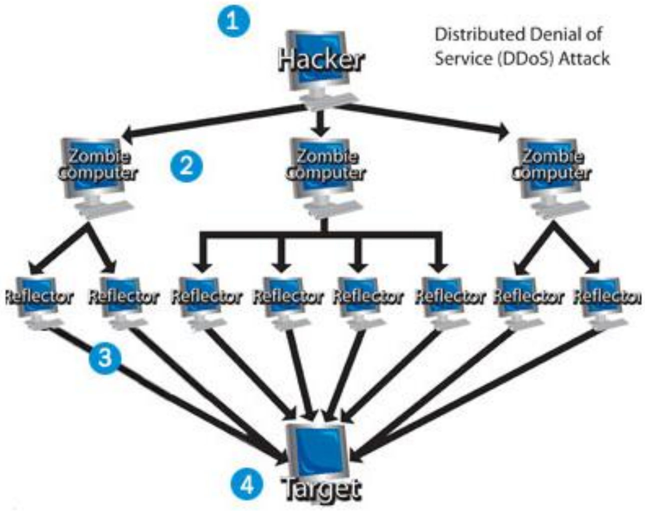

Figure 4: DDOS - Source: HowStuffWorks.com (2007)

It is recognized that DDOS attacks can cause disruption which will result in revenue losses when it comes to electronic commerce. According to

Brustoloni (2002) denial of service attacks can damage electronic commerce & business in two ways; the first if the website is down which means that the business cannot serve its customers the merchant would lose sales revenues. In addition to that, depending on the size of e-commerce the merchant “might” lose advertisements which would mean more loss. Secondly this “may affect” the behaviour of customers and advertisers since they will likely to look for alternatives. Marchany and Tront (2002) say that DDOS causes no damage to the seller’s website and it is simply overwhelming the access paths with incoming packets. When those attacks focus on e-commerce retail type of websites, the site will be unable to process the transactions and its reputation will be affected by DDOS attack also. According to Beal (2005) “script kiddies” are sometimes responsible from those attacks. And the reason of those attacks are usually “ego boosting. The term “script kiddie” is actually a negative term. Script Kiddie refers to hackers who use scripts or software of professional hackers instead of theirs since Script Kiddies lack of skill and knowledge to write their own software. However script kiddies are a big problem not only for e-commerce websites but to all sorts of networks. In year 2000 a 15 year old high school boy started DDOS attacks on sites such as E-Bay and Yahoo (Technopedia, 2003: Successtories, 2012). Those attacks cost more than 1 billion USD to the world economy. On the other hand this is a rare case but still, this example shows the seriousness of the danger for E-Commerce websites, especially for the “big ones” (Technopedia, 2003: Successstories, 2012).

2.3 VULNERABILITIES

According to both Hasan and Sobhan (2012) and (Sengupta, Mazumdar and Barik, 2005) There are three points of vulnerability about the E-Commerce.

- Client Side
- Server Side
- Communication Channel Side

2.3.1 CLIENT SIDE

Client Side security measures are to protect the privacy of the user. Also new technological solutions include protecting the user from malicious content. (Hasan and Sobhan, 2012). Sengupta, Mazumdar and Barik (2005) explains that before the use of active content web pages were actually “static” and static web pages could not do anything more than display the content. However “active content” changed this. According to Janssen (2014) “Active content is a type of interactive or dynamic website content that includes programs like Internet polls, JavaScript applications, stock tickers, animated images” He adds that developers use active content to visually improve a website and/or add new functionalities. Sengupta, Mazumdar and Barik (2005) adds that active content can display moving graphics, play audio etc. *In electronic commerce, active content is mainly used for shopping cart.* However embedding those contents into a web page paves the way for breaches and other threats. “Trojan Virus” which is very dangerous and it can begin to execute when active content is activated. Trojan virus is also part of malicious codes. According to Beal (2014) the term “malicious codes” are actually a “broad category” that includes worms and backdoors or other malicious active content.

2.3.2 SERVER SIDE & COMMUNICATION CHANNEL SIDE

In electronic commerce, there are transactions and payments. So physically, the place where those transactions and payments occur is the ‘’server’’ which actually contains the virtual things; such as the website, payment channel and even the customer database. Server side security is actually about protecting the machine(s) and the web-server from harm (Hasan and Sobhan, 2012).

Sengupta, Mazumdar and Barik (2005) explain that “the server” is the third link between the user and the electronic commerce server and every server has weaknesses and vulnerable points for those who are skilled enough and have the intention for it. Web server threats do not have a high risk. However, if the software is very complex then there is a chance that there will be some bugs and possible points for a security breach. Also, Sengupta, Mazumdar and Barik (2005) add that the e-commerce server responds user(s) browser requests along with the web server. But an e-commerce server is only designed for web service. These bugs and weaknesses may provide “holes” for the hackers to enter. In addition to those “threats” one of the most important threat for a server is “database threats” (Rafiq, 2014). E-Commerce platforms keep customer information in a database for many reasons.. This also includes product information also kept in databases and this is connected to the web server. If a hacker somehow acquires this information, valuable information will be at risk. Communication Channel side refers to Security Triad. These are Confidentiality, Availability and Integrity. The communication channel side is actually related to privacy since integrity and confidentiality is directly connected to privacy although they do not represent the same thing.

2.4 PRIVACY

Ferraro (1998) claims that privacy and security is not the same thing unlike many individuals who say otherwise. According to Merriam Webster Dictionary (2014) (1) ‘’Privacy’’ is the quality or state of being apart from company or observation. (2) Freedom from unauthorized intrusion. And the ‘’Security’’ is (1) the quality or state of being secure. (2) Measures taken to guard against espionage or sabotage or crime attack, escape (Ferraro, 1998). Head & Yuan (2001) talked about the same difference between security and privacy. They claim that there is still much ‘confusion’’ in security-community between these concepts and ‘’Privacy requires security because without security the information privacy cannot be protected’’

Privacy is a concern to Electronic Commerce. According to Ackerman & Davis (2003) ‘’Privacy as a business issue is extremely sensitive to changes in the surrounding context’’. They add that changes in people’s expectations can alter business issues. They think that the ‘’technical environment’’ is changing and business opportunities are present in this environment. Use of digital systems leads to a higher rate of data capturing therefore this allowed e-commerce sites to collect huge data about the customers, such as ‘’personal preferences’’. Ackerman & Davis (2003) add that new techniques allows ‘’data mining’’ for buying patterns. It is possible to use this data for to create ‘’personalized e-commerce’’ and this gives a better online shopping experience for a customer. The reason of this is because the websites which have personalised e-commerce services make recommendations to the customer depending his/her past shopping history such as page views and past purchases (Joseph, 2006). Also personalized e-commerce can improve the customer support and/or the experience on a specific web site. Explaining this; Dhillon & Moores (2002) *say* that the reason of these collection methods is actually the competitive business environment. This business environment forces businesses to collect huge amounts of personal information. Of course there may be a good intent about this since businesses want to customise their products for the benefit of the customer. According to Armstrong & Culnan (1999) there are two types of concerns about the privacy

No #	**Concern**
1	Unauthorized access to personal data
2	Re-use of data

Table 7: Concerns, Adapted from (Culnan & Armstrong, 1999)

As seen of the *table X* consumers are concerned about the unauthorized access to their personal data and the re-use of data. Re-use of data means secondary use, which means using a personal data for an irrelevant purposes (without consumer approval/permission) *(Culnan & Armstrong,* *1999)* Head & Yuan (2001) says that Privacy protection is a complex issue. The reason is there are two sides of this issue. One side is technical. The other side is about economics, social, legal issues that involves other parties. Businesses want to use IT to collect data from customers which includes their ''preferences''. Of course the reason for it is ''making profit'' However this might result in a violation of customers' privacy.

A framework has been developed by Head & Yuan (2001). This framework explains the situation about privacy and all involving parties in the process.

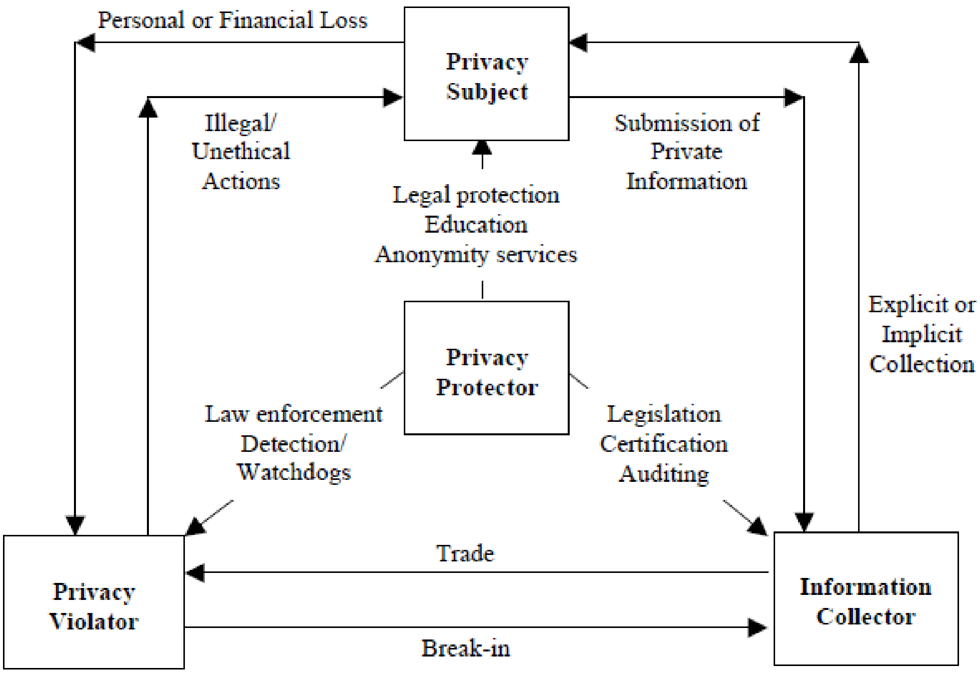

Figure 5 - Framework for Privacy Protection in Electronic Commerce, Taken from: Head & Yuan (2001)

Privacy Subject can be an organization or simply can be an individual who has legal rights. Mostly it is an individual, who do not want his/her information to be shared with third parties. (Head & Yuan, 2001) **Information Collector** is an individual or an organization that gathers data from ‘’privacy subjects’’ After the private data being collected, it is information collectors responsibility to secure this data. For example: financial Institutes hold important data (financial) of their customers. (Customers can be also companies) (Head & Yuan, 2001). **Privacy Violator** is an individual or an organization that illegally collects and distributes private information. This also includes ‘’the seller’’. If a company sells personal-private information illegally, (without permission) the company who sell this information will become a ‘’privacy violator’’ (so as the buyer) (Head & Yuan, 2001). “**Privacy Protector** can be government or other agencies who aims to protect the privacy”. (Head & Yuan, 2001) Cavoukian (1998) says that, the internet is an open communication system, which make it ‘’inter-operable. However Cavoukian (1998) adds that this made it vulnerable to certain risks such as hacking’’ According to Laudon & Traver (2013) Significant sites are hacked and those sites lost control over information of customers.

2.4.1 Privacy Issues and Objectives

A research-experiment conducted by Salehnia (2002) identified the concerns about privacy and what to do to make it better. A brainstorming session was conducted with panellists. Findings were the concerns about the Information Systems Privacy. A total of 114 concerns were found. After some adjustments, the total findings number downed to 85 objectives and within them the five most important issues were identified as:

Rank No#	*Issue (Objective)*
1	Companies should not sell personal information.
2	Prevention to theft of personal information by third parties.
3	Elimination of ‘’Losing Personal Files’’
4	Preventing hackers from destroying the data by ‘’maximizing security’’
5	Eliminate Spam

Table 8: 5 ‘’Privacy Issues and Objectives’’ (Adapted from Salehnia, 2002)

According to Selis et al. (2001) Most of consumers do not realise that there are some fundamental operations that allows free flow of personal data while they are enjoying the benefits of them. Customers who have high time-awareness rely on products that are customised. These products (or services) require high tech data collection. This includes buying-selling stocks and/or reaching bank accounts easily (Selis et al. 2001). The reason of this ‘’reliability’’ is the easy-computerized interactions among businesses. Selis et al (2001) add that those interactions give businesses means to build big data bases, which actually help businesses by targeting effectively and expand the market for the products (or services) businesses provide. Because of this information is being sold and/or shared with other parties, lots of consumers finds that their personal information are being used in many ways they may not have expected. Personal information includes financial data also, which includes credit card numbers bank balances etc. This information may end up (exposed to) parties that consumers do not have any relationship with (Selis et al. 2001). This actually proves the importance of reading Privacy Policies. Because most of the cases it is customers fault since they quickly press the “I have read, understood, and agree to the terms and conditions” button.

McDonald and Cranor, (2008) examined how much time it would take an individual to read the privacy policies in their work: *“The Cost of Reading Privacy Policies”* Annual estimates (findings) show that it takes 244 hours for an individual to completely read privacy policies and it takes 154 hours to skim.

Figure 6 – Privacy Statement Image

2.4.2 Security / Privacy Policies & Security Awareness

When an individual uses the internet, it is difficult to protect the anonymity. Udo (2001) says that users are ‘’partly responsible’’ to maintain privacy. Users should look for a privacy statement once they enter a website. Udo (2001) thinks that websites also should offer an option to restrict or limit the use of personal information (PrivacyRights, 2000). states that reputable websites have a section called ‘’Privacy Policy’’ It is possible to find out if the website (merchant) shares information with a third party. It is also possible to find out ‘’how those information shared with others’’ However this information may be in a separate policy which is most likely in ‘’security policy’’ and that also includes the merchant’s data security practices. According to Ciocchetti (2007) an electronic privacy policy is a written description posted on a company’s website, which explains how information provided by the visitors of the website are stored and/or being used by the business. McDonald & Cranor, (2008) explains the reason of importance about the privacy policy; without a privacy policy, there is no possibility that customers can know if an e-commerce website will be ‘’spamming’’ them when customers give their e-mail address. With a privacy policy, customers can examine the privacy protection before engaging with the site. (McDonald & Cranor, 2008).

3.0 METHODOLOGY

3.1 RESEARCH DESIGN & STRATEGY

> *"Research design" is different from the method by which data are collected"   (De Vaus, 2001)*

Burns & Grove (2002) define research design as "as a blueprint for conducting a study with maximum control over factors that may interfere with the validity of the findings." According to Conrad and Serlin (2011) the research design is widely used in education although it has different meanings in different studies. For example in one study, the research design can contain many sections such as a literature review, methods and conclusions. However, in another study it may reflect only the methodology part (Conrad and Serlin, 2011). Before beginning data collection, some pre-knowledge about the research topic was gained. However some researchers believe that it is better to enter the field without reading the literature, because there was a belief that pre-knowledge about the field would "taint" the researcher and makes the researcher to impose his/her preconceptions on the data (Elliott and Timulak, 2005). Still, the "pre-knowledge" was a great help for this study, since the questions of the survey and interviewee selection have been shaped by that knowledge.

One research question is based on the "literature review" in this study. Other one is based on the objective of this study.

- What are the main issues of E-Commerce, that affect consumers' online shopping choices

- How and why do those issues alter the consumers' method of payment.

3.1.1 Explanatory Study & Qualitative Methods

"An explanatory study sets out to explain and account for the descriptive information." The "descriptive" method is usually for to answer *"what"* type of questions, explanatory research asks *"how and why"* (Gray, 2004). In addition to that the goal of explanatory research is broader than descriptive research (McNabb, 2002). In this research, the relationships between the issues and respondents examined in a way that only descriptive method cannot exactly answer. Because in explanatory research, key variables and key relationships are defined. McNabb (2002) claims that explanatory research methods interpret cause and effect relationships between variables. Descriptive research methods would not be interested in the relationships between those variables. Mwape and Mumba (2012) state that explanatory can be a continuation of descriptive research. Because this type of research "goes beyond" and explaining why the problem(s) are occurring. De Vaus (2001) adds that "good description" actually provokes the "why" questions and he concludes that the purpose of explanatory research is to go beyond the descriptive study.

McNabb (2002) says that the explanatory research is the approach taken in many qualitative researches.

Purpose of the Study - Explanatory	**General Research Questions**
• To explain the patterns related to the phenomenon question • To identify plausible relationships shaping the phenomenon	• What events, beliefs, attitudes or policies shape this phenomenon? • How do these forces interact to result in the phenomenon?

Table 9: Explanatory Description – Source: (Marshall and Rossman, 1989)

According to Jansen (2010) there is a distinction between pre-structured and open-ended surveys. In pre-structured survey, aspects, categories etc. defined in advance while in open-ended survey those aspects are not defined. However Jansen (2010) claims that "qualitative researchers identify qualitative research with *induction* and excluding the analysis of pre-structured data". Elliott and Timulak (2005) say that the research questions leading to collection of qualitative data are usually open ended in nature. The survey conducted in this research intended to be qualitative because some questions focus on "perception of the respondents" and using a *deductive approach* and focusing on raw numerical data would have limited this research because there "may" be some factors that influence the results such as cultural differences since respondents are from different countries (Turkey and UK). Because of that a subjective analysis is intended. *Quantitative* research uses an objective approach while *qualitative* research uses a subjective approach to gather data for reflecting “perceptions” (Mwape and Mumba, 2012). According to Gray (2004), using an *inductive approach,* data is analysed to see if the relationship between variables becomes visible. On the contrary, the *deductive approach* generates hypothesis about those variables. Depending on the evidence the hypothesis either accepted or rejected. Unlike quantitative analysis, *“qualitative analysis requires some creativity, for the challenge is to place the raw data into logical, meaningful categories”* (Hoepfl, 1997)

3.2 Interpretivism as a Research Paradigm

Paradigm means “a theory or a group of ideas about how something should be done, made, or thought about” (Merriam-Webster, 2014). Guba et al. (1994) say that a paradigm can be viewed as a set of basic beliefs that deals first principles. Paradigm actually originates from the Greek paradeigma and late-Latin; *paradigma.* (Merriam-Webster, 2014).

According to Myers and Avison (2013) there are three categories of paradigms for qualitative research, these are: *Positivist, Interpretive and Critical*. In addition to those, Guba and Lincoln (1994) suggested that there are four categories, by adding post-positivism.

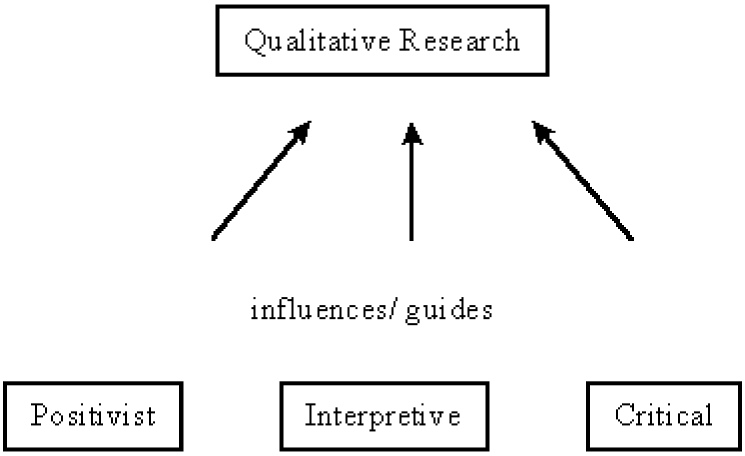

Figure 7 – Philosophical Assumptions. Source: Myers and Avison, 2013

Orlikowski & Baroudi, (1991) and Myers & Avison (2013) explained that "Positivist studies serve primarily to test theory" in order to attempt to increase predictive understanding of the phenomena. However Interpretative research in Information Systems area *"aimed at producing an understanding of the context of the information system, and the process whereby the information system influences and is influenced by the context" (*Myers & Avison, 2013).

This research is based on Interpretivism since the qualitative research method is chosen. As explained in first part of the methodology, in this research there are perceptions of respondents and relationships between concepts because of that a subjective route is taken. Interpretative researchers believe that the best way to learn about people is to be flexible and *subjective* in one's approach (Rubin and Babbie, 1989). In addition to that, Kroeze (2011) states that the interpretivism is a philosophical system and focuses reality as a human-construction, for that interpetivism can be understood subjectively.

3.3 Data Collection

3.3.1 Primary Data

Questionnaires and Interviews prepared after the research about literature review is completed. De Vaus (2001) thinks that some researchers design their questionnaires and/or interviews too early "before thinking through what information they require to answer their research questions." De Vaus (2001) adds that the conclusion will be weak because of that reason, as it will not be convincing and will therefore fail to answer the research questions.

3.3.1.1 Interviews

According to Harrell and Bradley, (2009) "Interviews are actually discussions and generally one on one between an interviewer and an individual meant to gather information on a specific set of topics." Cohen, Manion and Morrison (2007) add that "the interview" is a flexible tool for data collection. They say that gathering data as in surveys or other experimental situations is actually the one of the purposes of an interview.

According to Gill et al. (2008) there are three fundamental types of research interviews:

- Structured
- Semi-Structured
- Unstructured

Structured Interview is based on a survey, asked in same order and method of all subject of research. Structured Interviews have little flexibility available to researchers (Edwards and Holland, 2013). Wildemuth (2009) adds that "structured interviews are very similar to questionnaires although these kinds of interviews are administered orally rather than in writing. If the researchers aware of what they don't know structured interviews are useful as Guba & Lincoln (1985) suggest. Also they say that "in unstructured interviews, if researchers are not aware of what they don't know they rely on the respondents to tell them." Wildemuth (2009) examined that lots of definitions of unstructured interview can be found in the literature. But all of them have a common point of "not having predefined question" Wildemuth (2009) adds that "just because this type of interview does not require pre-defined questions does not mean that they are random and non-directive." Harrell and Bradley (2009) say that researcher has minimum control over the respondent(s) since the researcher cannot control the conversation. However, semi-structured interviews are different. In this type of interview "a guide is used with questions and topics that must be covered" (Harrell and Bradley, 2009).

Two unstructured interviews were conducted for this particular research. The first Interview was conducted with a "*Fraud Officer*" who works for a Bank in the United Kingdom. The second interview was conducted with a "*Shop Owner"* who has been doing business online and recently opened a store and turned his business into a "bricks and clicks" type in Turkey.

In order to protect their anonymity and privacy, respondents addressed as Interviewee X and Interviewee Y in this paper.

Interviewee	Title/Job-Sector	Country
Interviewee X (Male)	Fraud Officer / Bank	United Kingdom (UK)
Interviewee Y (Male)	Shop Owner / Clothing Store	Turkey (TR)

Table 10 – Interviewees, Titles and Countries

3.3.1.2 Survey (Internet Based)

Zhang (2000) claims that the internet has provide more efficient and effective ways to conduct surveys compared to traditional means. Emde & Fuchs (2012) states that web surveys are self-managed and it is up to the respondent to transform the response to its final format.

In this research, “if yes” and “if no” options have not been used in surveys. According to Cohen, Manion and Morrison (2007) forcing respondents to use a yes or no format results would increase “positive answers” because if respondents do not have any idea or they are neutral about the item “they may choose yes rather than no.” Dillman et al (2003) examined this problem that and found out that internet based questionnaires have higher percentage of positive answers compared to paper-based questionnaires.

Roztocki (2001) says that the most significant advantage of internet based survey is its speed. Another advantage is “the reach” (Roztocki, 2001).

Type	Country	Language of the Survey
Survey (15 questions)	Turkey (TR)	Turkish
Survey (15 questions)	United Kingdom (UK)	English

Table 11 – Survey Table

“Reach” was crucial for this research. The reason for it is; focusing on two countries at the same time would be time consuming and costly if the traditional survey method was picked. Roztocki (2001) examined that Internet-based surveys effectively reaches respondents in different geographic areas. He added that those advantages make internet-based surveys practical.

3.3.2 Secondary Data

Observations, interviews and surveys are not always enough. Secondary data has its advantages and can be more accurate and/or relevant than primary data (Crawford, 1997). Secondary data is used in order to support the findings of the primary surveys and interviews in this research. Some of this data includes European Union and Google data.

EU data comes from Eurostat – *a website where its main role is to process and publish comparable statistical information* - (Eurostat, 2014). Since statistical authorities in EU member states collect the data for some purposes, data is reliable. Reliability for data is very important in both primary and secondary research. Crawford (1997) says that an evaluation of the “source” is needed when it comes to secondary data since there are things to consider such as source bias, reliability and time span.

4.0 RESULTS

In this section, results of the survey take up most of this section; also the results of interviews were discussed together with the survey results. In addition to those, secondary data is included in some of the charts/figures in order to reinforce the primary data.

4.1 Turkey, United Kingdom and the European Union

The purpose of this section is to compare Turkey and the United Kingdom together with the European Union about online shopping/e-commerce in order to have a better understanding of the online shopping situation of those countries among the others in the same continent. The reason of choosing the United Kingdom for this study is the UK has the highest share of market in e-commerce business. (Retailresearch.org, 2014). The reason of choosing Turkey for this study is sociological since *"Turkey is both European and Middle Eastern at the same time"* (Nadolski, 2008).

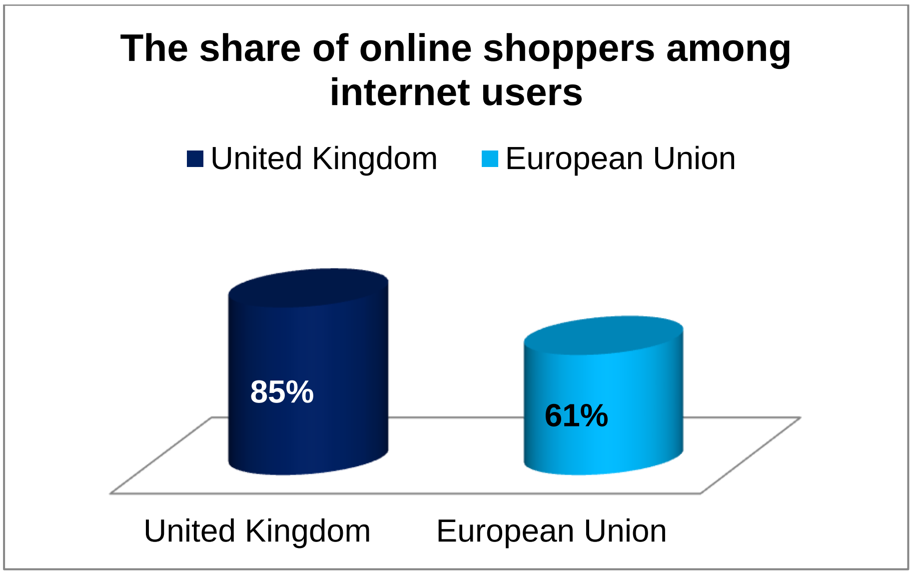

Figure 8: Online Shoppers / Internet Users - Source: Eurostat, 2013

According to Eurosat (2013) online shopping is very popular in the EU. The share of online shoppers among internet users varies between the EU member countries. The United Kingdom has the highest proportion. Computer use in United Kingdom is very high compared to European Union average and Turkey. When it comes to E-Commerce, a comparison is needed between the United Kingdom and Turkey since this paper focuses on both rather than the European Union. The United Kingdom is an EU member country and Turkey is an official EU candidate country[2]

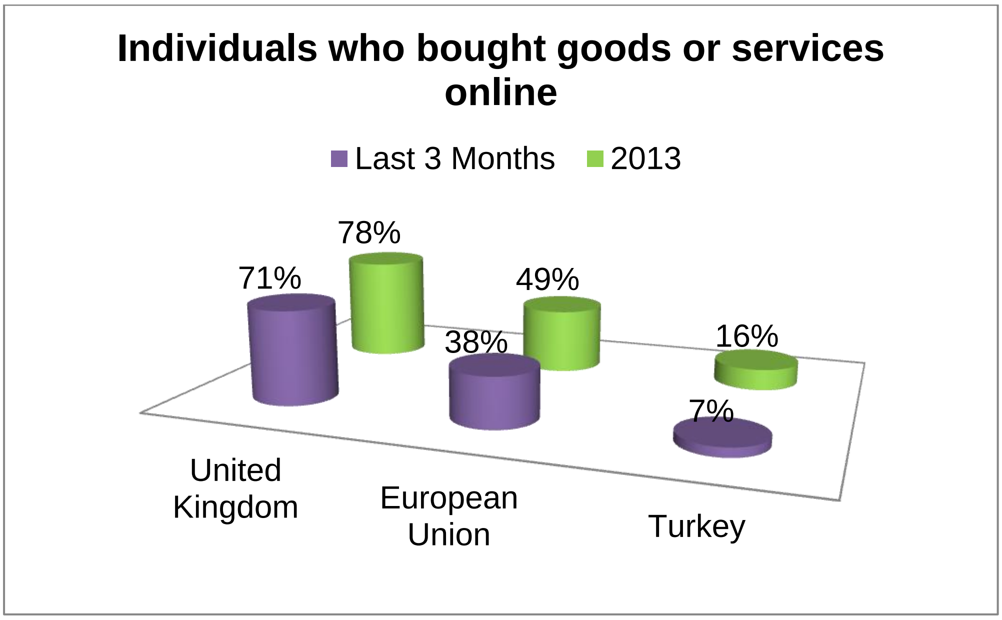

Figure 9: Individuals who bought goods or services online - Source Eurosat (2014)

Figure X shows the individuals having ordered/bought goods or services for private use over the Internet in the last three months. Like the previous graph about "share of online shoppers among internet users" the United Kingdom

[2] Helsinki European Council, December 1999

has the highest percentage of Europe. Turkey is 7% which is very low compared to the UK and the wider European Union. Turkey is second-lowest in all Europe, while Romania[3] is the lowest with 5% (Eurosat, 2014).

4.2 Age, Gender and Device Data (Survey)

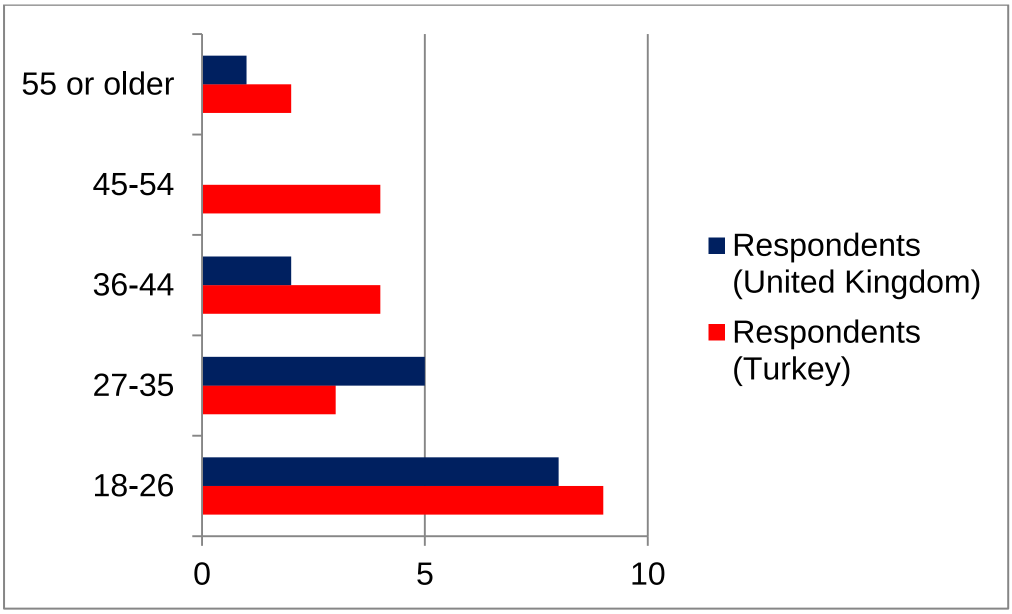

Figure 10 – Age of Respondents

Figure X shows the respondents' age for both Turkey and the United Kingdom. There are total 38 respondents, 22 from Turkey 16 from the United Kingdom. This means 58% of respondents are Turkish, and 42% of respondents are British. People were chosen depending on two criteria, first criterion was the respondent should be either Turkish or British. The second criterion was making sure the respondent shops online. The majority of respondents are between the ages of 18-35. This can be explained by the online shopping statistics/demographics.

[3] Not included on the table

Adults (18+) were targeted for this particular survey since there can be some complications about online payments if someone is under eighteen in both countries. According to Turkish Civil Code (2002) Article 11, “the age of majority is eighteen (full)” As for the United Kingdom; In England and Wales legal age is eighteen. For example if a citizen under eighteen applies to a bank for a credit card, his/her application would be turned down since in England and Wales people under eighteen usually cannot be held responsible about the contracts they make. However in Scotland the majority age is 16 in most cases. “Age of Legal Capacity (Scotland) Act 1991” states that “from age sixteen a person has full legal capacity to enter any form of agreement” (Legislation.gov.uk 1991; Citizens Advice Bureau 2014)

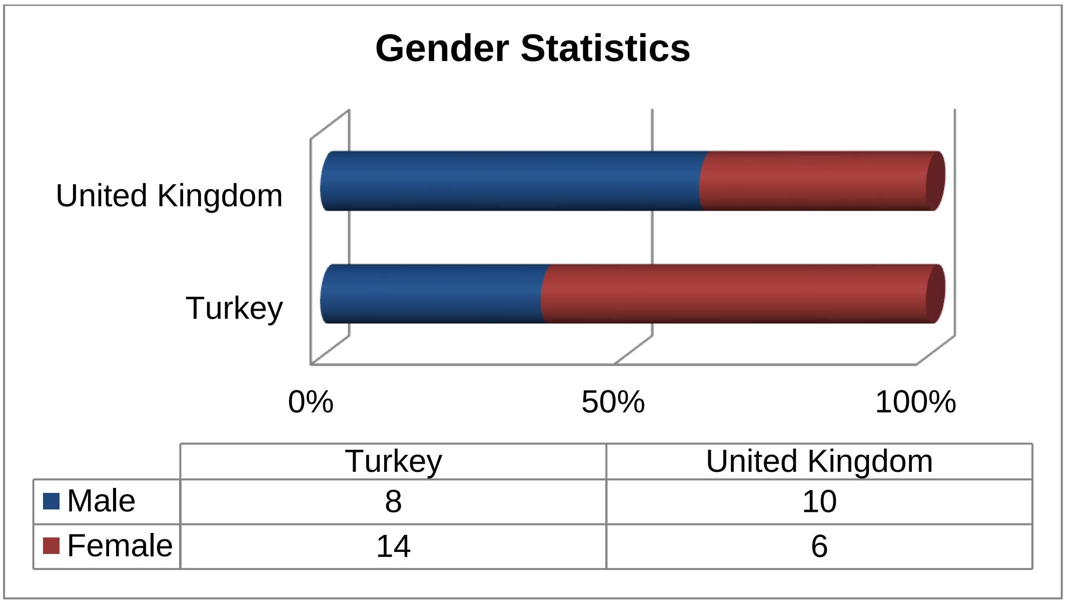

Figure 11 – Gender Stats

While looking for respondents for this survey, gender was not a criterion. As a result male and female numbers are not balanced. The percentage of male participants in United Kingdom is 63% and female participants are 38%. As for Turkey; the majority of respondents are females which are equal to 64%

and the rest are males which are equal to 38%. Interestingly gender affects the results in this survey since there are significant differences between males and females about “trust”.

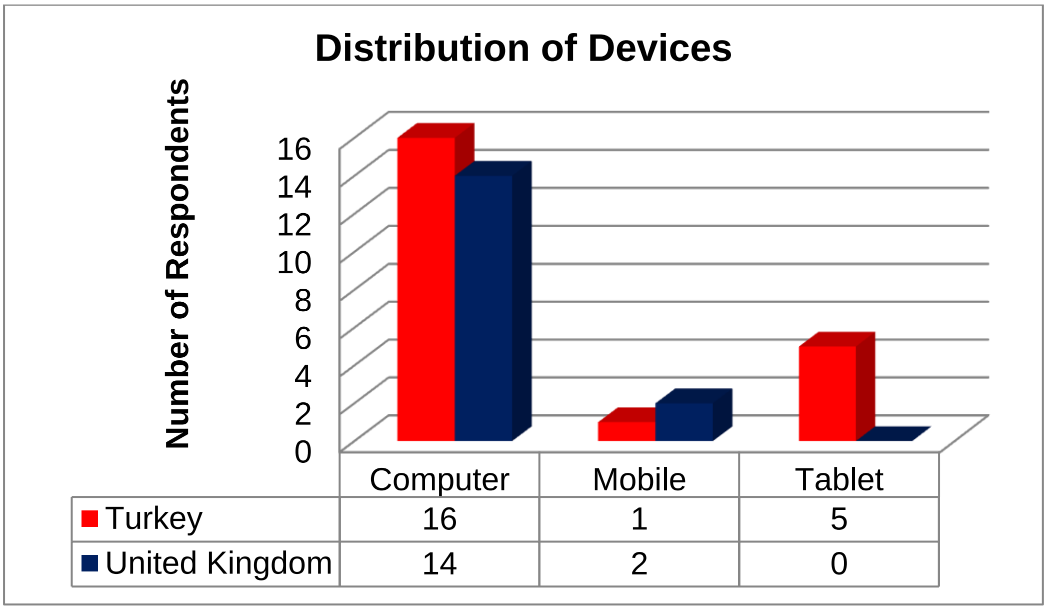

Figure 12 – Device Distribution

This survey demonstrates that the percentage of people who use a computer for online shopping is very high. 88% of the respondents in United Kingdom use computer for online shopping and 12% use mobile. No respondent uses a tablet in the UK, this might have happened actually by chance since the respondent number is very low and it may exclude some people with particular devices. Turkey is almost the same as the United Kingdom in that, the majority of respondents use a computer (laptop or desktop) for online shopping. 5 respondents use a Tablet for e-commerce, which is an interesting result because 5 respondents equals 23 per cent among the respondents in Turkey, while the rest 73% use a computer and 4% use a mobile for online shopping.

4.3 Privacy and Security

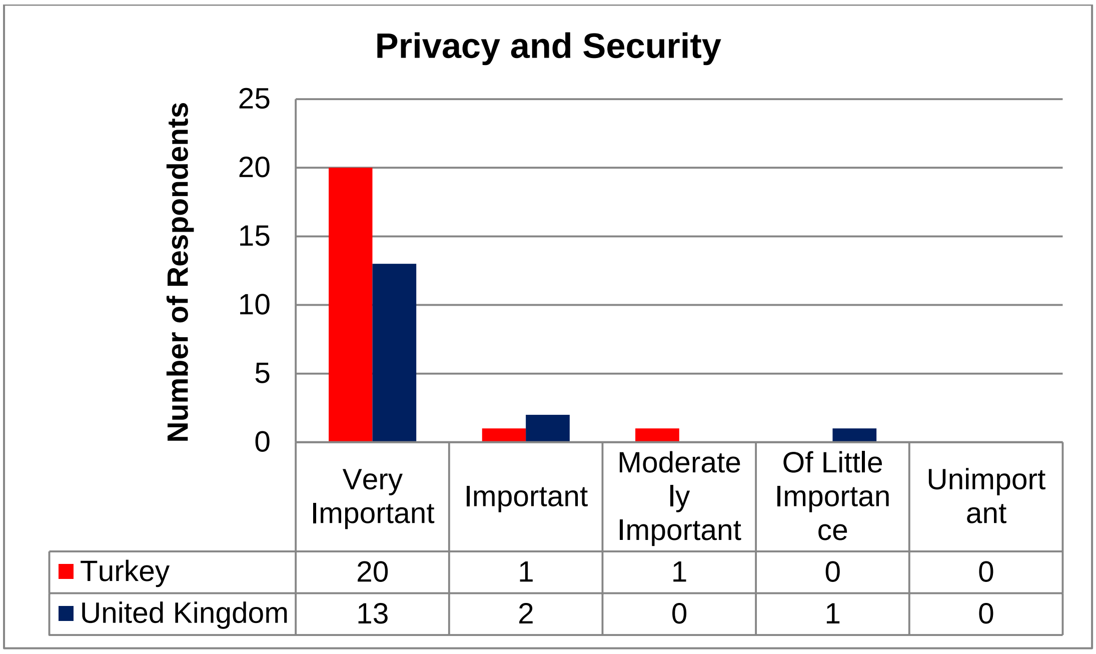

Figure 13 – Importance of Privacy and Security

As in the literature review part, security and privacy is proven to be the most problematic issue in electronic commerce. Results show that overall, 97% per cent of respondents of this survey find privacy and security as vital concepts in E-Commerce. By contrast the “importance level” may be different to person to person. The *Figure 13* shows that 91% of respondents find privacy and security as a “very important concept” while 3% find as moderately important and 4% as important. Only one respondent found that security and privacy has a little importance for E-Commerce.

These results about the security aspects of E-Commerce also include people's perspective of scams. Scams and transaction security is somewhat complicated, an interview conducted with a "Fraud Officer" which this study refers him as "Interviewee X".

The interview with "Interviewee X" was based on scams and frauds about payments and payment systems. In addition to those, the problems they cause to customers and how it affects the bank. Interviewee X claimed that one of the top problems about payment security is ***social engineering.***

4.4 SOCIAL ENGINEERING

Atkins and Huang (2013) identify "social engineering" as "a psychological exploitation which scammers use to skilfully manipulate human weaknesses and carry out emotional attacks on innocent people" Interviewee X identified social engineering as "tricking people to give their information". Interviewee X added that there are several methods of social engineering. Firstly, Interviewee X discussed the issues of "*phishing*" and "*spoofing".* According to Atkins and Huang (2013) "phishing is a growing area of Internet fraud with the number of victims on the rise" Interviewee X stated that customers are complaining about fake e-mails and malware. In addition to those Interviewee X mentioned *"telephone banking impersonation".*

Leena, (2011) reports that a lot of e-mail is being sent where the source of the identity of the e-mail is changed. Sending e-mails convinces the receiver so he stays unaware of the real sender. E-Mail spoofing is an important phase for scamming because e- mail spoofing is the way of launching phishing attacks to people. The email attackers' goal is to get information about the particular user such as passwords (Pandove, Jindal and Kumar, 2010). Interviewee X explained that when a customer (victim) clicks on the particular link, the customer is redirected to a fake website and the website can often look like it is the official website of the trusted organization (in his case it is a bank). He added that some customers cannot distinguish between a fake website and the official one because of “the theme” (look and feel) of both websites looks exactly the same. Pandove, Jindal and Kumar (2010) explain this by giving an example: a phishing e-mail is actually a disguised e-mail from a trusted organization such as a bank. The sender seeks to get sensitive information by tricking the receiver with the fake website. Spoofed e-mails may also include malware, viruses or both. Interviewee X said that the institution he works for warns customers about this issue. Pandove, Jindal and Kumar (2010) add that some e-mails contain malware. When e-mails come from a trusted source, users do not think that the e-mail may be spoofed and click the link or download the attachment. Some attachments have malware and/or Trojan virus which cause much bigger problems. Hughes and DeLone (2007) explained that Trojan horses are dangerous and destructive programs and add that there are some technical differences between worms, viruses and Trojans and those terms often confused with one another. Hughes and DeLone (2007) add that Trojan horses may perform harmful actions such as deleting files, stealing important information such as passwords, and Trojans are capable of opening a backdoor which allows hacker to control the computer, this can be used for performing DDOS attacks by hackers.

4.5 Website Design

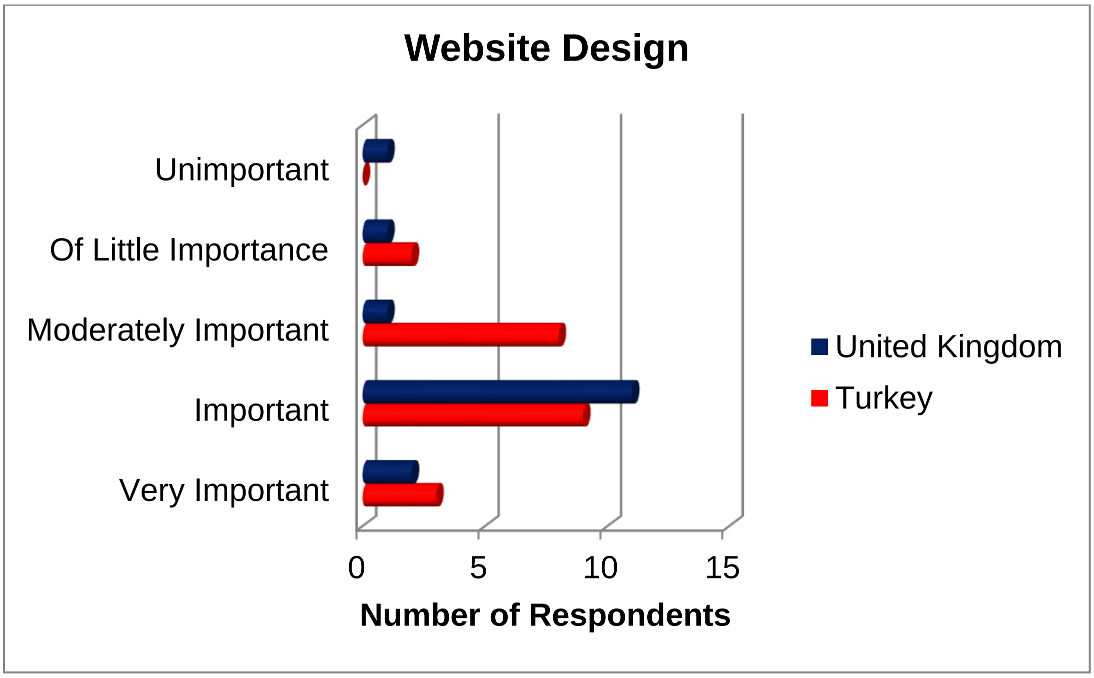

Figure 14 – Design of Website

The purpose of the question about the website design was to find out if it has an effect on customers about trust and payment. Respondents from the United Kingdom found the website design to be more important than the respondents from Turkey. 13% found the concept of website design as very important, whilst 69% found that the website design is important and 6% found it to be moderately important. By contrast, in Turkey 14% found that the website design is very important and 41% just important. The difference is actually about the percentages of important-moderately important. 9% respondents in Turkey found that website design has a little importance while 36% found that it is moderately important. In general people in Turkey found the design of website “less important”. Turkey has a slightly higher percentage about “very important”, However 69% of respondents in the UK found that the website design is important, which is actually very high compared to Turkey's 41%.

According to CreativeBoom (2011) the design and the layout should come first when building trust and bad design or layout will make people think that the products being sold on the website lacks style. According to Al-Slamy (2008) an E-Commerce business has four different components to build business to consumer and all those elements combined give a store ''personality''

These are: Product Catalogue, Shopping Cart, Transaction Security and Order Processing. (Al-Slamy, 2008)

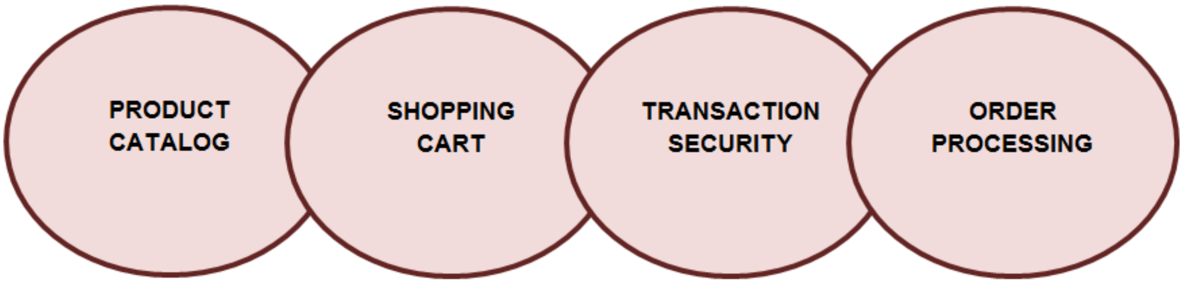

Figure 15 – Four Different Components; Adapted from Al-Slamy (2008)

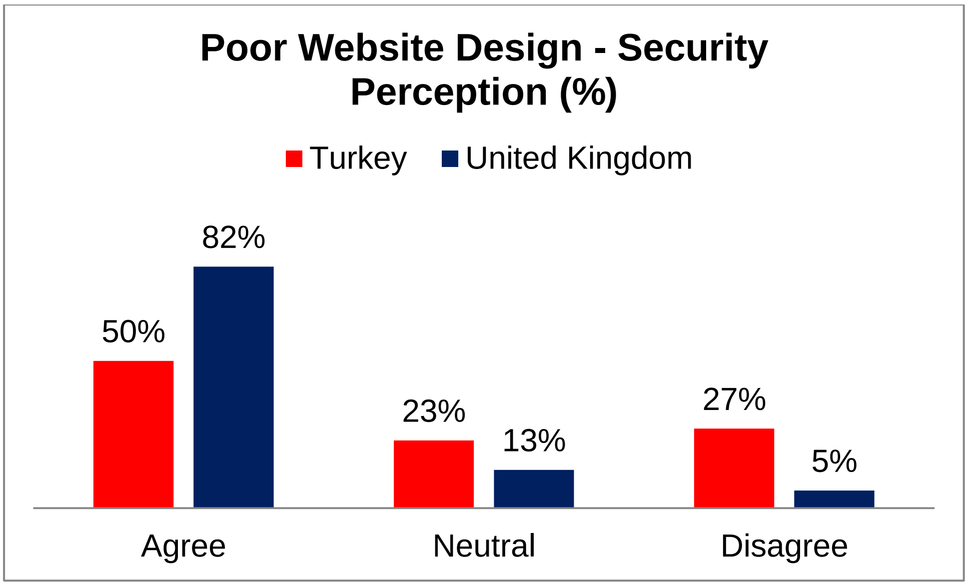

Figure 16 - Website Design and Security Perception

Respondents were asked if a poor website design or a bad interface would give them a bad impression about a website's security. The majority of people surveyed agreed about this, however there are significant differences between Turkey and the United Kingdom. Only half of respondents from Turkey agreed that poor website design would give them a bad impression about a website's security while 82% respondents from the United Kingdom agreed this would be important. 23% of respondents from Turkey and 13% of respondents from the United Kingdom are neutral about their perceptions which equals 19% overall.

These results show that the website design is a major determinant of their perceptions of security and trust in a website. On The Internet, customers cannot look a salesman in the eye or cannot touch the products. Pictures or videos of products and the promises are the things that customers rely on. If customers do not trust those promises and images, they will shop elsewhere (Reichheld and Schefter, 2000). Also, Rios and Riquelme (2008) state that “online businesses are mainly tangible and therefore it is difficult for consumers to judge them from tangible cues. They add that trust plays a critical role in this type of business compared to brick and mortar businesses where consumers can interact with physical things to establish trust (Rios & Riquelme, 2008).

Some websites such as Amazon and E-Bay established trust with consumers. The graph below shows if respondents “completely trust” websites such as Amazon and E-Bay. The phrase “completely trust” was intended in the question because of the possibility that people who participated in survey would say yes/agree since it wouldn’t be an absolute question.

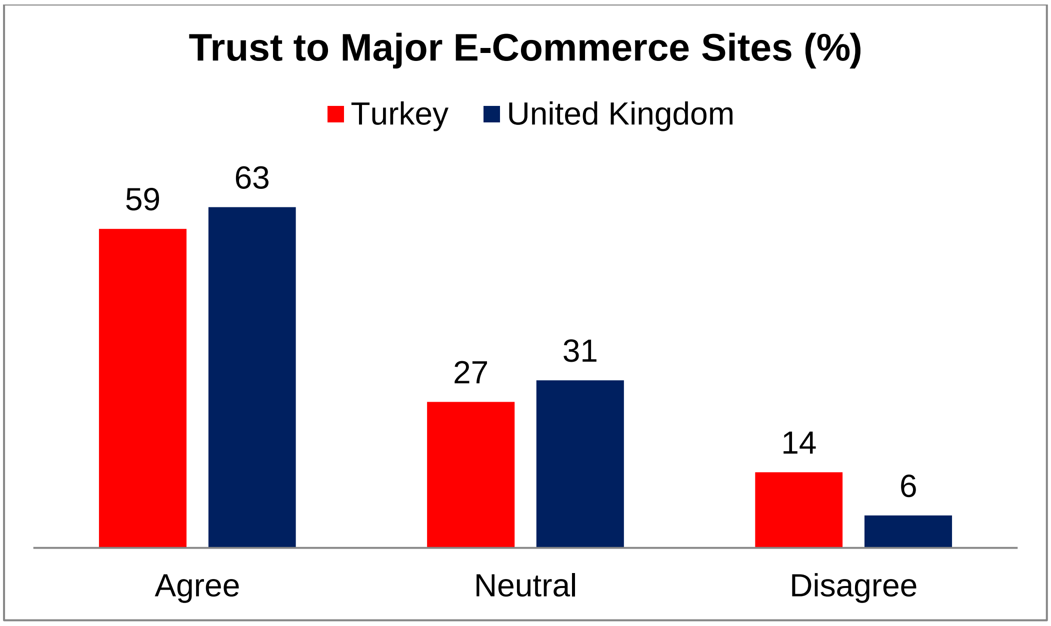

Figure 17 – Trust to Major E-Commerce Sites

59% of respondents from Turkey responded that they “completely trust” major online shopping sites such as Amazon and eBay while 63% of respondents from United Kingdom feel same. These results are very similar to each other, although there is a small gap between Turkey and the United Kingdom about neutral and negative answers which is worth mentioning. 14% of respondents from Turkey disagree while it is 6% in the United Kingdom. A total of 15 respondents (both countries included) do not trust major e-commerce sites completely, which is equals 39% which is a significant number. In contrast, since the phrase “completely trust” was used, it is somewhat unlikely that the results show the real perspective of consumers about Amazon and eBay overall. In addition to that, a Likert scale approach was used in the survey to counter this, although this may be the reason for too many “neutral” responses that caused inaccuracy. These results give an insight into the perspective of customers towards major e-commerce sites like Amazon and eBay since it is still positive overall.

Amazon actually “dominated” on line market by creating most the reliable website in the business. (Reichheld and Schefter, 2000). Customers feel very comfortable about sharing their information, which includes their real life addresses credit card information etc. But that if it were otherwise, if customers did not trust Amazon it would have been different since customers would not be sharing their personal info (Reichheld and Schefter, 2000). According to Gopalkrishnan (2007), trust between buyers and sellers is key to success and the strategy of eBay lies in trust to build e-loyalty. Srinivasan, Anderson and Ponnavolu, (2002) explain e-loyalty as “the customer's favourable attitude toward an electronic business, resulting in repeat purchasing behaviour”.

4.6 E-Wallet

Qin (2009) says that E-Wallet is commonly used payment option in E-Commerce. Only electronic currency can be stored in e-wallet. Usually, the users of e-wallets have to open account(s) at the banks. According to Jung and Jang (2014) e-wallet provides a means of maintaining important information such as e- currency, credit card data and passwords. Jung and Jang (2014) add that e-wallets are actually like real wallets because both wallets maintain important information about the user. Electronic wallets are protected by passwords and encrypted to prevent unauthorized use. Hackers use Trojan horses to collect wallet passwords. (Parsons and Oja, 2011). Heffernan (2005) says that “the e-wallet is an electronic version of credit or debit card” In order to make internet purchases, the money needs to be transferred from the bank account of the user to the e-wallet.

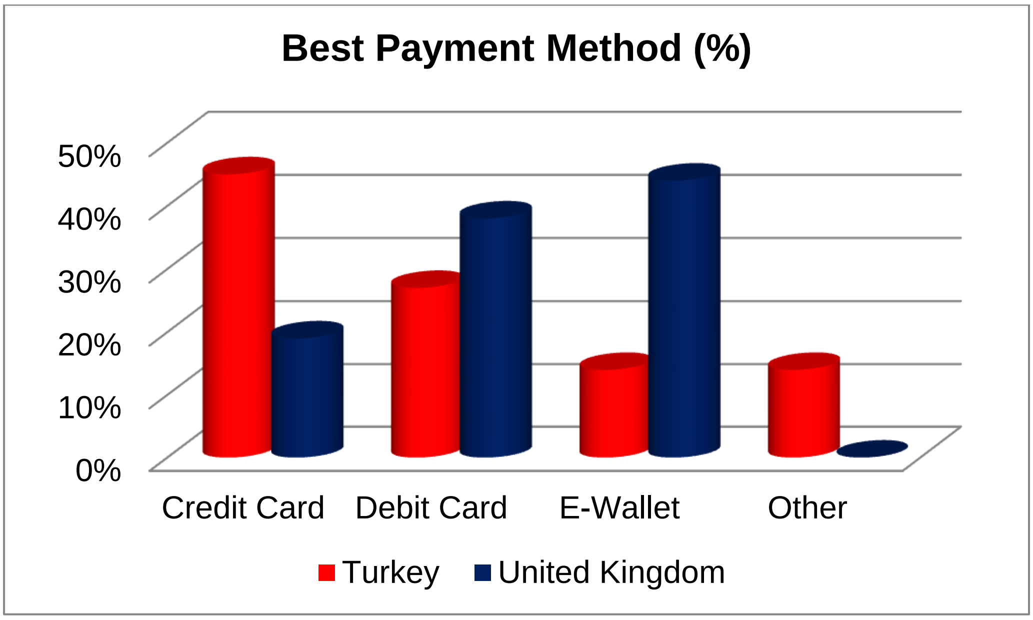

Figure 18 – Best Payment Method

There are huge differences between Turkey and the United Kingdom about payment methods. 45% of respondents from Turkey replied that paying with Credit Card is the best method for them while only 19% of respondents from the United Kingdom replied that according to them the best payment method is credit card. About debit card, the results are not too much different, but respondents from the United Kingdom think that a Debit Card is better than Credit Card; however respondents from Turkey think that Credit Card is better for them. Perhaps the more interesting result, 44% of respondents from the United Kingdom think that E-Wallet is the best payment method while 14% of respondents from Turkey think that it is the best method for online payment. There are many differences between Turkey and the United Kingdom when it comes to E-Wallet. Respondents were also asked if they find difficulty to learn and/or use E-Wallet.

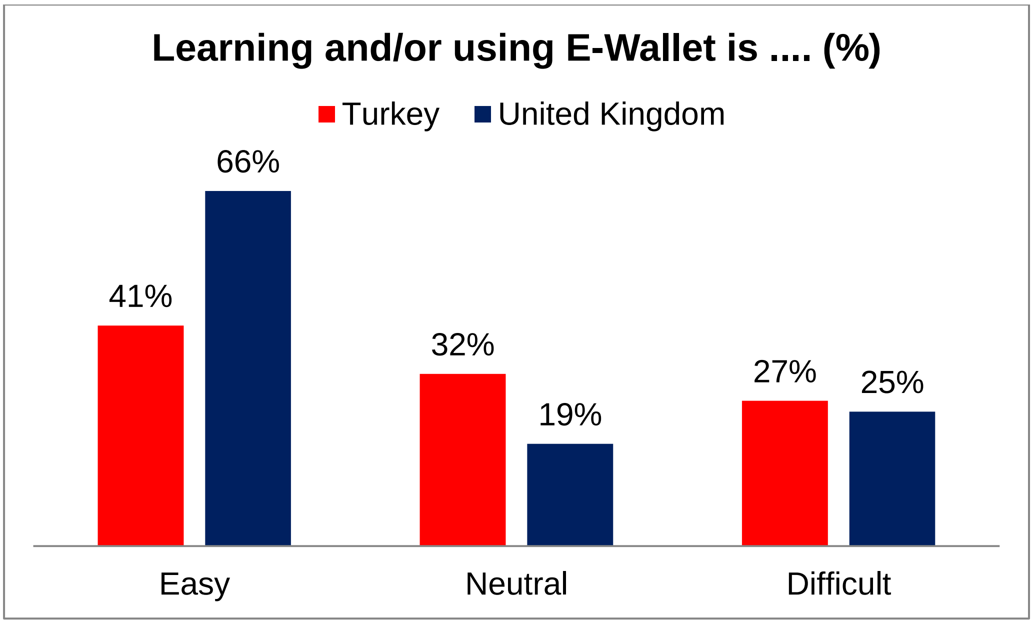

Figure 19 – Learning & Using E-Wallet

The figure above demonstrates the reasons for differences between Turkey and the United Kingdom about why E-Wallet choices were different on the previous figure. 66% of respondents from the United Kingdom found that using E-Wallet is actually easy. On the other hand only 41% of respondents from Turkey found that using E-Wallet is easy and 32 per cent of Turkish respondents remain neutral which is a high number. In total of 59% of Turkish respondents find E-Wallet difficult to use or learn. These numbers clarify the reason for a low percentage of Turkish respondents since very few numbers of respondents found that E-Wallet is the best payment method because of learnability and usability.

The United Kingdom is actually the opposite. 44% of respondents from United Kingdom found that E-Wallet is the best method for online payment and the figure clarifies it since 2/3 (66 per cent) of respondents from the United Kingdom found that E-Wallet is easy to use/learn. To sum up, respondents from Turkey either does not know how to use E-Wallet, and/or do not think it is easy to learn. Using PayPal or that kind of services might require some knowledge about computers and the internet. Turkey’s low percentage and the United Kingdom’s high percentage can be the reason of internet usage amount of both countries.

4.7 Internet Usage

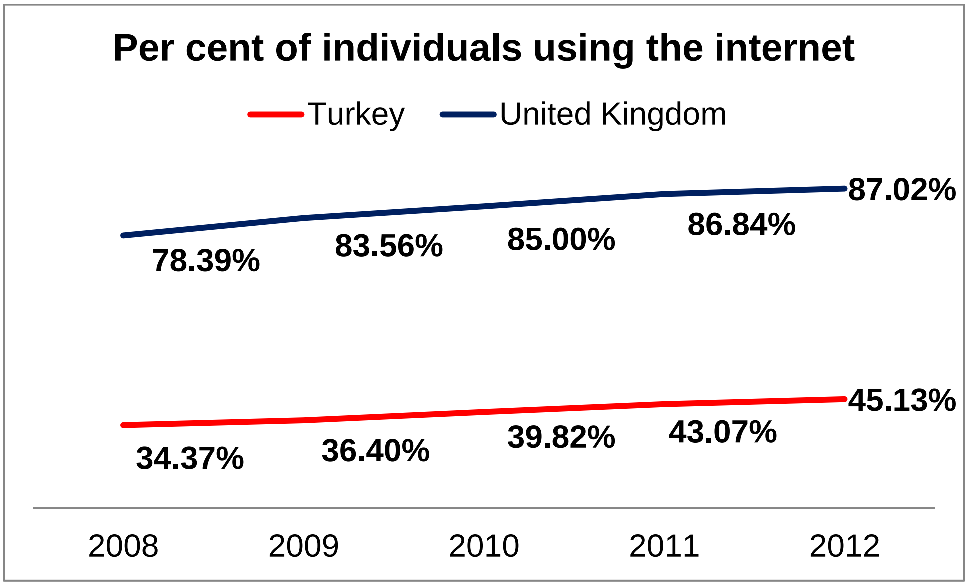

Figure 20 – Per cent of individuals using the internet. Source: (Google Public Data, 2012)

As can be seen on the Figure 20, there is a huge difference between Turkey and the United Kingdom about per cent of individuals using the internet. The most recent internet usage data on Google Public Data was the data of year 2012. Since 2012 is the most recent data, this research is based on these data. There are up-to-date sources about internet usage, however since Google is a trusted source using this data may give more accurate results.

45.13% per cent of individuals use internet in Turkey In summary, around half (50%) of population in Turkey use the internet while around 90% population use Internet in the United Kingdom.

Paying with E-Wallet is more complicated than paying with credit or debit card since there are some processes in E-Wallet. Qin (2009) say that those processes do not take more than 20 seconds, and those processes include form(s) that needs to be filled and finally, receiving the electronic receipt.

Majority of people find E-Wallet difficult, Olsen, Hedman & Vatrapu (2011) explains that *learnability* is very important when it comes to E-Wallet. They say that “It should be possible for the user to work out how to use the E-Wallet” and claim that people do not like spending their time in order to learn how to use a new payment system. Olsen, Hedman & Vatrapu (2011) identified four overarching goals about “Electronic Wallets”. These are*: Efficiency, Learnability, Utility and Safety.*

Olsen, Hedman & Vatrapu (2011) explains “*Efficiency”* as carrying out a task in E-Wallets. An E-Wallet should be efficient. If paying with an E-Wallet requires too much steps or long process, it would not be efficient. Olsen, Hedman & Vatrapu (2011) states that total steps of payment process in E-Wallets should not be more than six steps. Bidgoli (2002) says that electronic wallets are very useful for people, who are shopping online frequently. Bidgoli (2002) adds that electronic wallets eliminate re-entering information on online forms which results in a more efficient and fast shopping experience. Regarding safety, the research study by Olsen, Hedman & Vatrapu (2011) concluded that the security is the most important concept for the users of E-Wallet. The result concurs with this survey.

4.8 Cash on Delivery vs. Online Payment

Two respondents from Turkey chose the “Other” option as an answer to the question about the “best payment methods” instead of choosing card payment or E-Wallet. The respondents specify that “cash on delivery” is the best method for online shopping. According to Frary (2003) “the other-please specify” option should only be used when the investigator has been unable to establish the prevalent categories. This was the reason for “*the other”* option and this option were absolutely crucial in order to spot this issue.

According to Miller (2008) “cash on delivery” is very good on paper (in principle), however he claims that there are lot of problems about this method. For example:

- The Buyer can be away from home when the delivery is made.
- The Buyer can be at home but do not have the cash.
- The Buyer can refuse the pay and can reject the shipment

The interview conducted with Interviewee Y was crucial to spot the advantages of *“cash on delivery payment method”*. Interviewee Y stated that he uses Facebook to reach customers and he did not set up a website for his business. He explained that in order to receive payments online, he needs to set up an in-house payment or third party payment system. Interviewee Y explained further that sales would drop if he chooses to implement online payment system to his business since he claimed “cash on delivery method” is one of the reasons that customers shop from him.

Interviewee Y explained the “system” of his online sales. He promotes his business on Facebook and receives customer orders from Facebook, E-mail or via Phone by having their contact number, address and of course the chosen product. (Phone option was added later after he opened a shop in Istanbul.) After that the product(s) delivered to the specified address by the delivery service that Interviewee Y has an agreement with. The customer pays to the courier, either by cash or debit/credit card since the delivery service allows such payment. Interviewee Y said that it is an advantage for him because the couriers carry POS (point of sale) machine with them, although if customer pays with credit card, receiving the money from the delivery service takes 30 days. Since the business is in Turkey and customers are mostly Turkish, they feel comfortable about this kind of payment as Interviewee Y claimed.

In Turkey, “Trust” seems a big problem about online payments, therefore also for businesses. Wissam Otaky, the Chief Financial Officer of MarkaVIP (an online e-commerce company based on selling fashion and lifestyle products in the Middle East) stated in an interview in Turkey, that he has a dream about “eliminating cash on delivery in Middle East and replace that with credit card and online payments.” He claimed that the reason that people choose the cash on delivery as their payment option is “trust”. He adds that “people in the Middle East still not used to do shopping online, and they are very hesitant about security”[4] Turkey is included in the Statistics/Chars about Europe, however when investigated culturally, “Turkey

[4] Interview with Wissam Otaky, February 2014: https://www.youtube.com/watch?v=rYBnbDm-xiI (Video Link)

have “several identities, one of which is Middle Eastern” (Altunışık & Kavli, 2005).

4.9 Trust

The results show that trust dependent on lots of things since it depends country to country, culture to culture. According to Kamoun & Halaweh (2012) “online trust is a multi-faced and context-dependent construct that involves cognitive, behavioural, psychological, and cultural and risk factors.” Bansal (2009) say that the “Key factor” about success in Business to Consumer (B2C) is trust. According to Bansal (2009) “Trust is a psychological state compromising the intention to accept vulnerability based on positive expectations of the intentions or behaviours of another” while Oxford Dictionaries (n.a) defines trust as; “believe in the reliability, truth or ability of”. Bansal (2009) adds that “Trust helps consumers overcome perceptions of uncertainty”

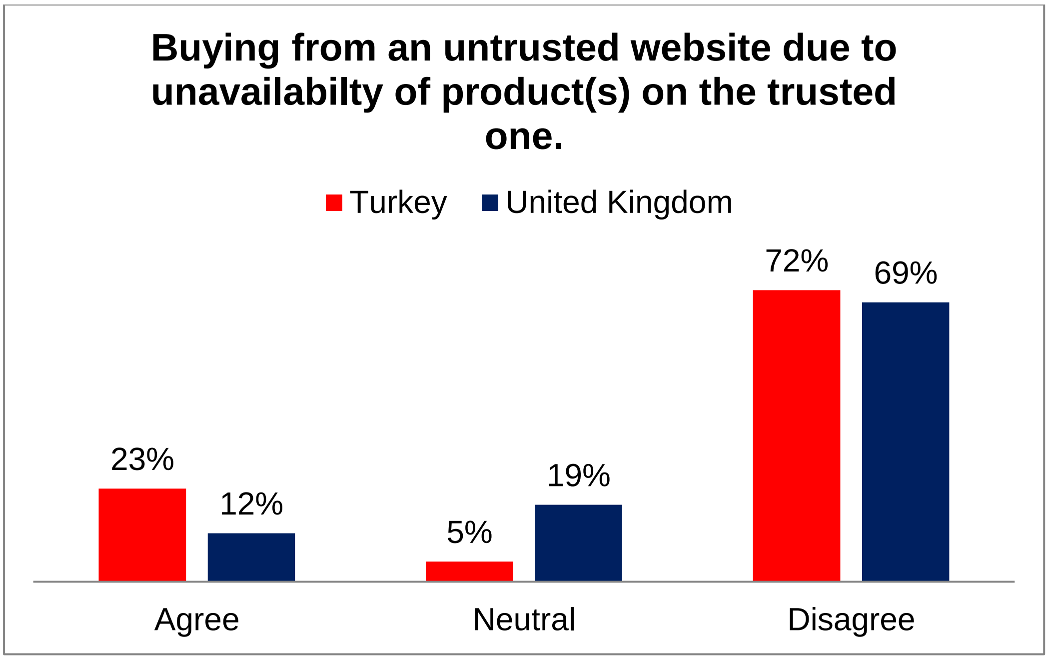

Figure 21 - Untrusted Website Purchase Chart

In total, only 23% of respondents from Turkey actually say that they would buy from a website that they do not trust if they cannot find the product or service they want to buy elsewhere, while only 12% of respondents from the United Kingdom agrees. Unlike other graphs, respondents from Turkey see this question as black and white, only 5% of Turkish respondents are neutral. Respondents from United Kingdom agrees less when compared to Turkish respondents however that difference seems to create a gap about neutrality between Turkey and United Kingdom while the majority of respondents from both countries disagreed. The result of this question is that the respondents overall, would not buy from a website that they do not trust if they cannot find the product or service they want to buy elsewhere. On contrary, there are some respondents around 18 % (overall) who would take this risk.

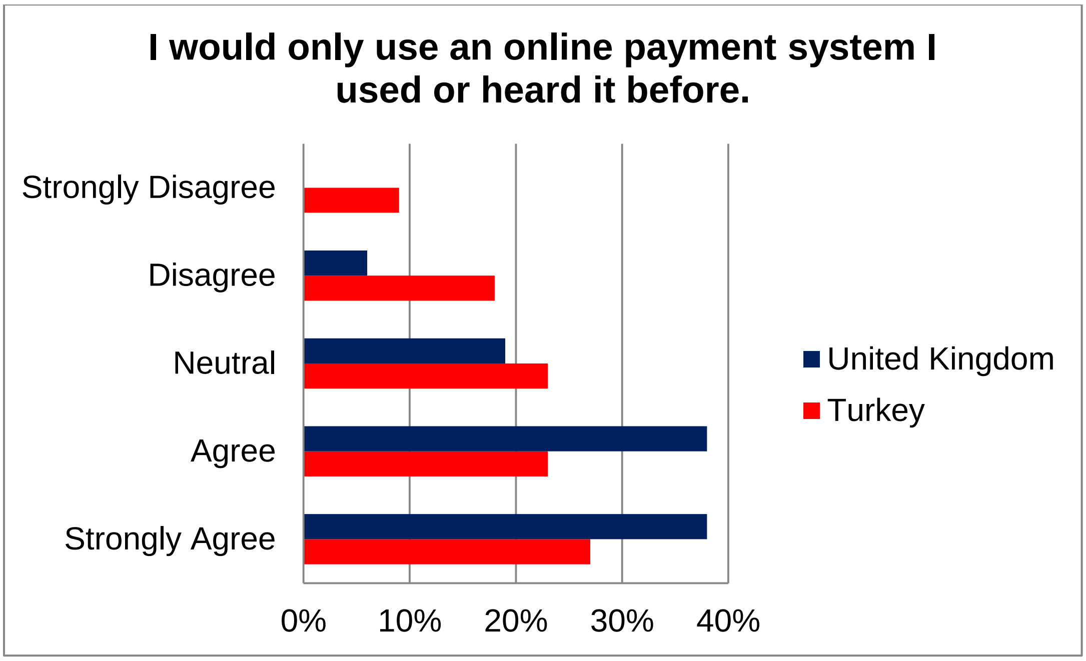

Figure 22 – New methods and Payment Choice

In Total of 50% of Turkish Respondents responded that they would use an online payment system that they used or heard it before. Interestingly, respondents from the United Kingdom seem to be more conservative about their choice of payment method. 72 per cent of respondents from United Kingdom either agrees (38%) or strongly agrees (38%) that they would use an online payment system that they used before. This means that the Turkish respondents are more open to learn and use new payment methods. There is neutrality around 21% overall, which I presume that those respondents either do not have any idea about their choices would be and they did not want to be absolute with their answers.

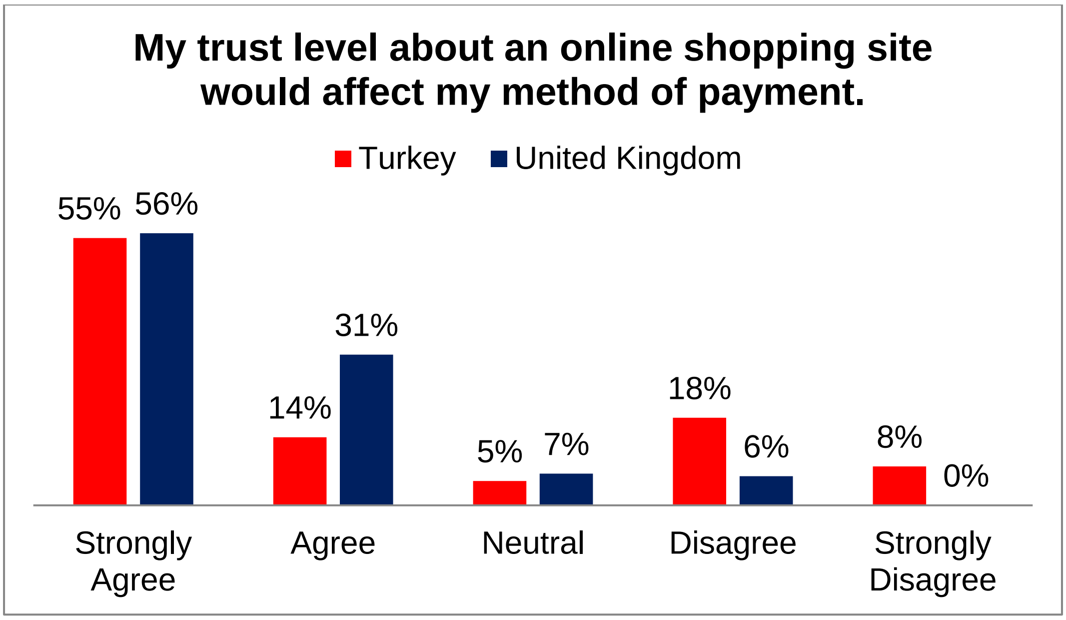

Figure 23 – Trust Level – Payment Methods

Figure X shows that 87 per cent of respondents from the United Kingdom agree that their level of trust for a website is a determinant of their choice for online payment. Overall 56% of respondents from United Kingdom "strongly" believe that their trust is a determinant for their choice of payment method(s). 55% of Turkish respondents also strongly agreed about this. Overall, Turkish respondents "agree less" since total "agree" percentage of Turkey is 69% while United Kingdom's is 87%. There is a very low neutrality for both countries; overall the neutrality percentage is below 7% *"*which means respondents have some idea about trust and they do know how it shapes/alters their choices*"* A total of 26 per cent of Turkish respondents and 6 per cent British respondents found that the trust has nothing to do with their payment choices. This can be explained by actually lack of knowledge of other methods since the learnability and usability of E-Wallet payment method percentage of Turkey was very low compared to United Kingdom. *Lack of knowledge of payment systems may force the online shoppers to rely* *on only one or two payment options, therefore "trust" cannot be a determinant at this point*. Some Turkish respondents do not want to change their payment method(s) and they find the new methods difficult to learn and/or use. Because results show that there are some Turkish respondents around 25-26% who "disagreed" a lot while only %6-7 of British respondents have the same mentality about trust and choice of payment method. On the other hand there is another factor that affects the payment method: ***Other Customers***

Respondents from both countries were asked if Customer Base and Social Media are important concepts for them.

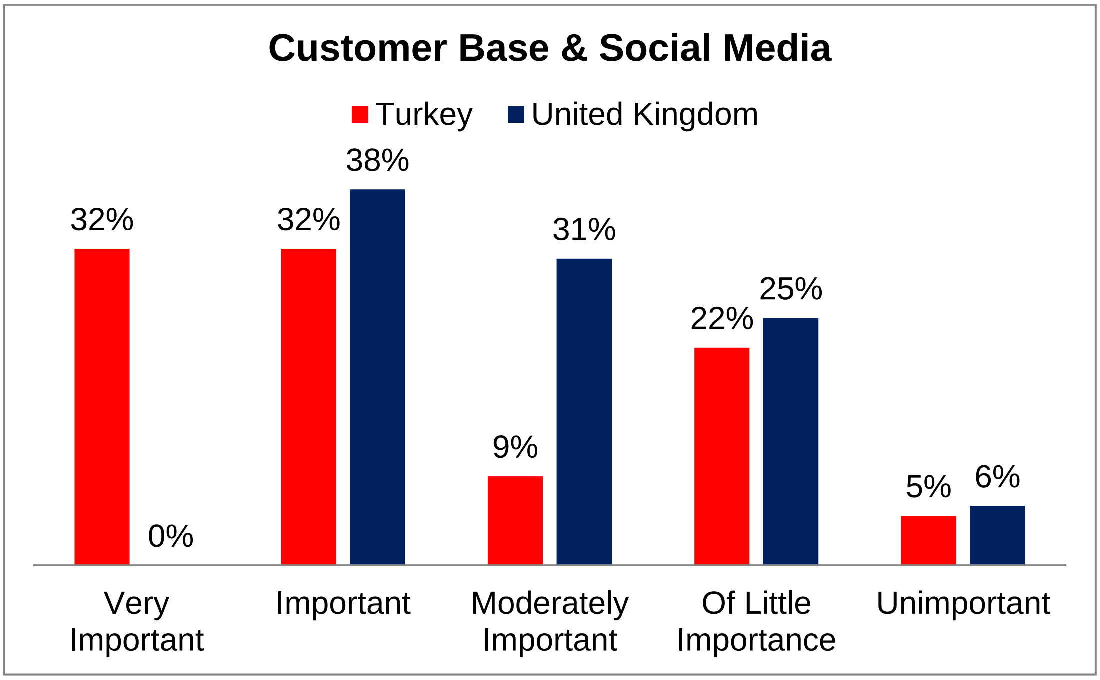

Figure 24 – Customer Base and Social Media

Results show that Social media has a huge effect on respondents from Turkey. In total, %64 found that social media is either very important (32%) or just important (32%). Interestingly, no respondent (0%) from United

Kingdom found customer base and social media as “very important”. Only 38% of respondents from the United Kingdom found customer base and social media important. In addition to that 31% found moderately important. As for Turkey only 9% found customer base and social media moderately important. In total, 27% of respondents from Turkey and 31% of respondents from the United Kingdom found customer base and social media has a little importance or unimportant for them.

Respondents were asked a similar question in order to spot if social media and what people say about specific e-commerce sites or products.

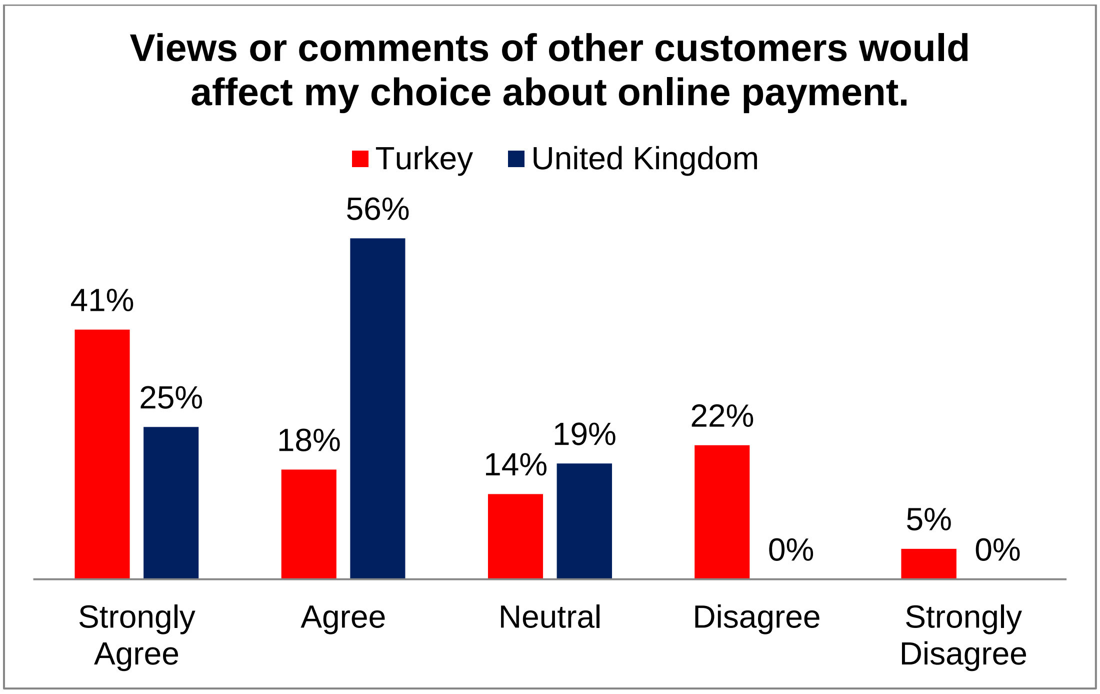

Figure 25 – Views of Customers and how it affects the payment choice.

Overall 34% of respondents strongly agreed that view of other customers would affect their choice about online payment. Another 34% just agreed while 16% remained neutral. Only 16% of respondents either disagreed or strongly disagreed. Some respondents from Turkey (41%) strongly agree that their choices will get affected by views of other people while 25% of respondents from the United Kingdom think the same. However in general, respondents from the United Kingdom agree more (81% vs., 59% of overall)

One of the “places” for finding out the views of other customers may be social media. Comments on social media can be positive, neutral or negative, and the results of the survey shows that respondents will likely to get affected by those comments. “Every business involved with social media will inevitably have some customer who gives negative comment” (O'Leary, Sheehan and Lentz, 2011). When it is positive, “nothing sells a product better than actual customer reviews and ratings of the products” (Singh and Diamond, 2012). Which may mean that depending on the marketing and/or strategy, customers can change their payment methods based on the reviews.

5.0 CONCLUSION AND RECOMMENDATIONS

Findings of this study show that security and privacy issues have a huge effect on trust. Since this study also found that trust is the determinant for a customer to shop from an online shopping site, also is a determinant of payment choice. In order to increase the security of the transactions and the trust level of the website, the payment process should provide the secure auditable mechanisms for automated electronic payment transactions (Patel, Mona & Taghavi, 2011).

This can be done in order to increase the trust level of consumers towards to a website. As the results and the literature review conclude that perception of security and privacy has a major effect on consumers about trust and this makes consumers to shift to another website or changing their payment method(s) to something more secure. *Consumers have to expose their private information in order to finish the purchasing process such as giving their credit card number, address etc (Zhang and Liu, 2011).* Privacy is the key driver of online trust, although depending of the category of the website this can be different since influence of trust changes. (Bansal, 2009). *Therefore electronic payment technology need to provide security mechanisms as a sufficient safeguards in the form of digital signatures, encryption and Web seal assurances…etc, (AL-ma'aitah and Shatat, 2011).*

For the technical side, there are certain things for website owners to make sure in order to have a more successful business. According to Smith (2004*) in order to prevent "denial of service" type of attacks there should be a comprehensive, tested business continuance plan to ensure that the E-*

commerce site can detect the problem. Literature review and results show that DDOS is a huge problem for e-commerce and this actually affect the consumer, which is related to the concept; *“availability of the website”* and causes lack of trust. “*Lack of trust is one of the most frequently cited reasons for consumers not purchasing from Internet vendors”* (Grabner-Krauter and Kaluscha, 2003). Of course the “availability of a website” is not the only determinant of trust since this study proved that there are other factors such as culture. Online shopping has a one big disadvantage because consumers cannot touch the products before they buy. In traditional shopping, consumers feel less *“uncertainty*” before they make a purchase decision (Zhang and Liu, 2011). As explained in the survey results part; consumer can visit a store for themselves and can physically touch the products in traditional shopping. In order to counter that disadvantage, putting high quality pictures and/or videos about products being sold on website may increase the “trust” , therefore increase the sales since respondents may see this a part of website design also. However there may other factors such as the history of website as in Amazon and eBay because Hiscock (2001) says that the main ingredient of a long term bond between consumer and a brand is “Brand Trust”. When brand trust is established, consumers may not be concerned with security and privacy issues as much as they concern on a random shopping website. However some problems may rise when an online shopping website is lack of focus. A lack of focus makes the loyalty process harder (Reichheld and Schefter, 2000). If an e-commerce website built too fast in order to “attract many customers as possible”, things might go wrong (Reichheld and Schefter, 2000). According to Reichheld and Schefter, (2000) the reason for that is executives often gauge their successes by page views, however that is not directly a business success. “The broader array of customers a company attempts to serve, the more complex the website becomes” (Reichheld and Schefter, 2000).

In the end, literature review and the results concluded that trust is the most important factor for consumers about online shopping and online payment. Security and privacy issues and also cultural factors affect consumers’ perception together since those concepts are “determinants” of trust as this study concludes. For those reasons*; “the future of business-to-consumer electronic commerce depends both on consumer trust toward Web retailers and also toward Internet technology.”* (Pavlou, 2001).

5.1 Recommendations for Future Research

This study has covered only two countries, samples from more countries and different cultures would make the future study more generalizable and applicable to others. Using a different methodology such as an experimental research method may provide better results. Because manipulating and controlling some variables might help in order to spot crucial points and/or anomalies since it is possible to influence the experiment with own observations depending on the hypothesis (Martin and Bateson, 2007).

6.0 REFERENCES

Ackerman, M. and Davis Jr, D. (2003). Privacy and security issues in e-commerce. New economy handbook, p.215.

AL-ma'aitah, M. and Shatat, A. (2011). Empirical Study in the Security of Electronic Payment Systems. IJCSI International Journal of Computer Science Issues, 8(4), pp.393-401.

Al-Slamy, D. (2008). E-Commerce security. IJCSNS International Journal of Computer Science and Network Security, 8(5), pp.340--344.

Altunışık, M. and Kavli, O. (2005). Turkey. 1st ed. New York: RoutledgeCurzon.

American Heritage Dictionary, H. (2002). The American Heritage Dictionary entry: firewall. [online] Ahdictionary.com. Available at: https://ahdictionary.com/word/search.html?q=firewall [Accessed 24 Aug. 2014].

Atkins, B., Huang, W. and others, (2013). A Study of Social Engineering in Online Frauds. Open Journal of Social Sciences, 1(03), p.23.

Bansal, A. (2009). Transcending horizons through innovative global practices. 1st ed. Indore: Prestige Institute of Management and Research.

Beal, V. (2005). Denial of Service (DoS) Attacks Explained - Webopedia.com. [online] Webopedia.com. Available at: http://www.webopedia.com/DidYouKnow/Internet/DoS_attack.asp [Accessed 28 Aug. 2014].

Beal, V. (2014). What is Malicious Code? Webopedia. [online] Webopedia.com. Available at: http://www.webopedia.com/TERM/M/malicious_code.html [Accessed 30 Aug. 2014].

Bidgoli, H. (2002). Electronic commerce. San Diego: Academic Press.

Bocij, P. and Chaffey, D. (2003). Business information systems. Harlow, England: FT/Prentice Hall.

Brightlabs, (2013). Is your electronic signature legally binding?. [online] Brightlabs.com.au. Available at: http://www.brightlabs.com.au/page/Blog/Is_your_electronic_signature_legally_binding/ [Accessed 23 Aug. 2014].

Brustoloni, J. (2002). Protecting electronic commerce from distributed denial-of-service attacks. pp.553--561.

Burns, N., Grove, S. (2002). Study guide for Understanding nursing research. Philadelphia: Saunders.

Cavoukian, A. (1998). Privacy: The Key to Electronic Commerce. [online] Information and Privacy Commissioner/ Ontario. Available at: http://www.ipc.on.ca/images/Resources/e-comm.pdf [Accessed 16 Aug. 2014].

Ciocchetti, C. (2007). E-Commerce and Information Privacy: Privacy Policies as Personal Information Protectors. American Business Law Journal, 44(1), pp.55--126.

Citizens Advice Bureau, (2014). Citizens Advice - Young people – money and consumer rights. [online] Adviceguide.org.uk. Available at: http://www.adviceguide.org.uk/england/debt_e/young_people_money_and_consumer_rights.htm [Accessed 10 Oct. 2014].

Cohen, L., Manion, L. and Morrison, K. (2007). Research methods in education. 1st ed. London: Routledge.

ComputerWeekly, (2011). The top five SME security challenges. [online] Computerweekly.com. Available at: http://www.computerweekly.com/feature/The-top-five-SME-security-challenges [Accessed 24 Aug. 2014].

Conrad, C. and Serlin, R. (2011). The Sage handbook for research in education. 1st ed. Thousand Oaks, Calif.: SAGE Publications.

Crawford, I. (1997). Marketing research and information systems. 1st ed. Rome: Food and Agriculture Organization of the United Nations.

CreativeBoom, (2011). Top 20 tips on how to build trust online | Creative Boom. [online] Creativeboom.co.uk. Available at: http://creativeboom.co.uk/tips/top-20-tips-on-how-to-build-trust-online/ [Accessed 16 Oct. 2014].

Culnan, Mary J., and Pamela K. Armstrong. (1999). Information Privacy Concerns, Procedural Fairness and Impersonal Trust: An Empirical Investigation. Organization Science, 10 (1): 104- 115.

De Vaus, D. (2001). Research design in social research. 1st ed. London: SAGE.

Dillman, D. A., Smyth, J. D., Christian, L. M. and Stern, M. J. (2003) Multiple answer questions in self-administered surveys: Joint Statistical Meetings 2003

Edwards, R. and Holland, J. (2013). What is qualitative interviewing?. 1st ed.

Elliott, R. and Timulak, L. (2005). Descriptive and interpretive approaches to qualitative research. A handbook of research methods for clinical and health psychology, pp.147--159.

E-Lock, (n.a.). [online] Available at: http://www.elock.com/pdf/Digital_Signature.pdf [Accessed 24 Aug. 2014].

Emde, M. and Fuchs, M. (2012). Using Adaptive Questionnaire Design in Open-Ended Questions: A Field Experiment. JSM Proceedings, Statistical Computing Section. Alexandria, VA: American Statistical Association..

Entrust, (2003). [online] Available at: http://www.entrust.com/wp-content/uploads/2013/05/digsig_transactions.pdf [Accessed 25 Aug. 2014].

Eurostat, (2014). What we do. [online] Epp.eurostat.ec.europa.eu. Available at: http://epp.eurostat.ec.europa.eu/portal/page/portal/about_eurostat/introduction/what_we_do [Accessed 8 Sep. 2014].

Ferraro, A. (1998). Electronic commerce: the issues and challenges to creating trust and a positive image in consumer sales on the World Wide Web. First Monday, 3(6).

Fienberg, S. (2006). Privacy and confidentiality in an e-commerce world: Data mining, data warehousing, matching and disclosure limitation. Statistical Science, pp.143--154.

Fillingham, D. (1997). 6.805/STS085: A Comparison of Digital and Handwritten Signatures. [online] Groups.csail.mit.edu. Available at: http://groups.csail.mit.edu/mac/classes/6.805/student-papers/fall97-papers/fillingham-sig.html [Accessed 23 Aug. 2014].

Frary, R. (2003). A brief guide to questionnaire development. Virginia Polytechnic Institute \& State University. Retrieved October, 9, p.2003.

Gibson, D. (2011). Understanding The Security Triad (Confidentiality, Integrity, and Availability) | Understanding the Security Triad (Confidentiality, Integrity, and Availability) | Pearson IT Certification. [online] Pearsonitcertification.com. Available at: http://www.pearsonitcertification.com/articles/article.aspx?p=1708668 [Accessed 31 Aug. 2014].

Gill, P., Stewart, K., Treasure, E. and Chadwick, B. (2008). Methods of data collection in qualitative research: interviews and focus groups. Br Dent J, 204(6), pp.291-295.

Gopalkrishnan, J. and Gupta, V. (2007). eBay:" The world's largest online marketplace"-A Case Study. Indian Institute of Management Kozhikode.

Grabner-Krauter, S. and Kaluscha, E. (2003). Empirical research in on-line trust: a review and critical assessment. International Journal of Human-Computer Studies, 58(6), pp.783--812.

Gray, D. (2004). Doing research in the real world. 1st ed. London: Sage Publications.

Gray, T. (2003). Firewalls: Friend or Foe?. EDUCAUSE review, 38(1), pp.60--61.

Guba, E., Lincoln, Y. (1994). Competing paradigms in qualitative research. Handbook of qualitative research, 2, pp.163--194.

Harrell, M. and Bradley, M. (2009). Data collection methods. 1st ed. Santa Monica, CA: RAND.

Hasan, R. and Sobhan, M. (2012). Study on e-Commerce Threats and Security. Laudon, K. and Traver, C. (2013). E-commerce. Boston, Mass.: Pearson.

Hasan, R. and Sobhan, M. (2014). Study on e-Commerce Threats and Security.

He, Q., Duan, Y., Fu, Z. and Li, D. (2008). Factors Affecting Online E-Payment Adoption. Web Technologies for Commerce and Services Online, 2008 1. SME B2B E-Commerce and Customer Loyalty Revisited, p.55.

Head, M. and Yuan, Y. (2001). Privacy protection in electronic commerce--a theoretical framework. Human Systems Management, 20(2), pp.149--160.

Heffernan S. (2005) Modern Banking, 1st ed. Wiley.

Hiscock, J. (2001). Most trusted brands. Marketing, 1(March), pp.32--3.

Hoepfl, M. (1997). Choosing qualitative research: A primer for technology education researchers. Digital Library and Archives of the Virginia Tech University Libraries.

HowStuffWorks.com, (2007). Distributed Denial of Service Attacks - HowStuffWorks. [online] HowStuffWorks. Available at: http://computer.howstuffworks.com/zombie-computer3.htm [Accessed 26 Aug. 2014].

Hughes, L. and DeLone, G. (2007). Viruses, worms, and trojan horses: Serious crimes, nuisance, or both?. Social science computer review, 25(1), pp.78--98.

InfoSSL, (2014). SSL Glossary - P. [online] Info.ssl.com. Available at: http://info.ssl.com/ssl_kb/article.aspx?id=10219 [Accessed 25 Aug. 2014].

ISA.co.uk, V. (2011). CIA triad - Information Security Adviser. [online] Informationsecurityadviser.co.uk. Available at: http://informationsecurityadviser.co.uk/cia-triad/ [Accessed 29 Aug. 2014].

Jansen, H. (2010). The logic of qualitative survey research and its position in the field of social research methods. 11(2).

Janssen, C. (2014). What is Active Content? - Definition from Techopedia. [online] Techopedia.com. Available at: http://www.techopedia.com/definition/4847/active-content [Accessed 1 Sep. 2014].

Joseph, P. (2006). E-commerce. New Delhi: Prentice-Hall of India Pvt. Ltd.

Jung, I. and Jang, G. (2014). A Secure and Reliable e-Wallet using a Smart SSD. Life Science Journal, 11(7s).

Karimov, F., Brengman, M., Van Hove, L. and Van, L. (201 1). The effect of website design dimensions on initial trust: a synthesis of the empirical literature. Journal of Electronic Commerce Research, 12(4), pp.272--301.

Khosrowpour, M. (2009). Encyclopedia of information science and technology. Hershey, PA: Information Science Reference.

Kroeze, J.H. (2011). "Interpretivism in Information Systems: A Postmodern Epistemology?," . Sprouts: Working Papers on Information Systems, 11(171).

Laverty, S. (2014). The Disadvantages of a Firewall. [online] Small Business - Chron.com. Available at: http://smallbusiness.chron.com/disadvantages-firewall-62932.html [Accessed 31 Aug. 2014].

Lee, M. & Turban, E. 2001. A Trust Model for Consumer Internet Shopping: International Journal of Electronic Commerce, 6(1): 75-91

Leena, N. (2011). Cyber Crime Effecting E-commerce Technology. Oriental Journal of Computer Science \& Technology, 4(1).

Legislation.gov.uk, (1991). Age of Legal Capacity (Scotland). [online] Available at: http://www.legislation.gov.uk/ukpga/1991/50/enacted [Accessed 1 Nov. 2014].

Lim, Y. (2003). Digital Signatures, Certification Authorities: Certainty in the Allocation of Liability. Sing. J. Int'l \& Comp. L., 7, p.183.

Lincoln, Y. and Guba, E. (1985). Naturalistic inquiry. Beverly Hills, Calif.: Sage Publications.

Marchany, R. and Tront, J. (2002). E-commerce security issues. pp.2500--2508.

Marshall, C. and Rossman, G. (1989). Designing qualitative research. 1st ed. Newbury Park, Calif.: Sage Publications.

Martin, P. and Bateson, P. (2007). Measuring behaviour. Cambridge: Cambridge University Press.

McCullagh, A. (2000). Non-repudiation in the digital environment. First Monday, 5(8).

McDonald, A. and Cranor, L. (2008). Cost of reading privacy policies, the. ISJLP, 4, p.543.

McNabb, D. (2002). Research methods in public administration and nonprofit management. 1st ed. Armonk, N.Y.: M.E. Sharpe.

MerchantSelect, (2001). MerchantSelect - The Complete Merchant Provider Resource. [online] Merchantselect.com. Available at: http://www.merchantselect.com/articles/?1000-3.html [Accessed 2 Sep. 2014].

Merriam Webster Dictionary, (2014). [online] Definition of Paradigm. Available at: : http://www.merriam-webster.com/dictionary/paradigm [Accessed 8 Sep. 2014].

Merriam Webster Dictionary, (2014). Privacy - Definition and More from the Free Merriam-Webster Dictionary. [online] Merriam-webster.com. Available at: http://www.merriam-webster.com/dictionary/privacy [Accessed 15 Aug. 2014].

Miller, M. (2008). Absolute beginner's guide to eBay. 5th ed. Indianapolis, Ind.: Que.

Mittal, A., Shrivastava, A. and Manoria, M. (2011). A Review of DDOS Attack and its Countermeasures in TCP Based Networks. International Journal of Computer Science \& Engineering Survey (IJCSES), 2, p.4.

Moores, T. and Dhillon, G. (2002). Do privacy seals in e-commerce really work?. Communications of the ACM, 46(12), pp.265--271.

Murray J. (2003). Public Key Infrastructure Digital Signatures and Systematic Risk,. 2003 (1) The Journal of Information, Law and Technology (JILT)

Mwape, B and Mumba, J. (2012) Tools for Policy Research, 1st Edition, AuthorHouse

Myers, M. (2013). General References on Qualitative Research. [online] Qual.auckland.ac.nz. Available at: http://www.qual.auckland.ac.nz/general.aspx [Accessed 8 Sep. 2014].

Myers, M. and Avison, D. (1997). Qualitative research in information systems. Management Information Systems Quarterly, 21, pp.241--242.

Nadolski, D. (2008). The etatist Turkish Republic and its political and socio-economic performance from 1980-1999. Lanham, MD: University Press of America.

Nesbit, T. (2001). What Do Pigs And Chickens Have To Do With eCommerce?.

NewYorkTimes, K. (2011). Stanford Hospital Patients' Private Data Was Posted Online. [online] Nytimes.com. Available at: http://www.nytimes.com/2011/09/09/us/09breach.html?pagewanted=all&_r=0 [Accessed 31 Aug. 2014].

Niranjanamurthy, M. and Chahar, D. (2013). The study of E-Commerce Security Issues and Solutions. perspectives, 2(7).

O'Leary, S., Sheehan, K. and Lentz, S. (2011). Small business smarts. 1st ed. Santa Barbara, Calif.: Praeger.

Olsen, M., Hedman, J. and Vatrapu, R. (2012). Designing digital payment artifacts. pp.161--168.

Orlikowski, W.J. and Baroudi, J.J (1991) Studying Information Technology in Organizations: Research Approaches and Assumptions, Information Systems Research, 2(1):1-8.

Ozkan, S., Bindusara, G. and Hackney, R. (2010). Facilitating the adoption of e-payment systems: theoretical constructs and empirical analysis. Journal of enterprise information management, 23(3), pp.305--325.

Pandove K , Jindal A , Kumar R (2010) Email Spoofing, International Journal of Computer Applications (0975 – 8887), Volume 5– No.1.

Parsons, J. and Oja, D. (2011). Computer concepts 2011. Boston, MA: Course Technology.

Patel, A., Qi, W. and Wills, C. (2010). A review and future research directions of secure and trustworthy mobile agent-based e-marketplace systems. Information Management \& Computer Security, 18(3), pp.144--161.

Pavlou, P. (2001). Integrating trust in electronic commerce with the technology acceptance model: model development and validation. AMCIS 2001 Proceedings, p.159.

PrivacyRights, (2000). Online Shopping Tips: E-Commerce and You | Privacy Rights Clearinghouse. [online] Privacyrights.org. Available at: https://www.privacyrights.org/online-shopping-tips-e-commerce-and-you#4 [Accessed 17 Aug. 2014].

Qin, Z. (2009). Introduction to e-commerce. 1st ed. Berlin: Springer.

Rachana C.R (2013) The Role of Digital Signatures in Digital Information Management: International Monthly Refereed Journal of Research In Management & Technology. Vol.2 ISSN–2320-0073.

Rafiq, M. (2014). Database Security Threats and Its Techniques. International Journal of Advanced Research in Computer Science and Software Engineering, 4(2).

Reichheld, F. and Schefter P. (2000). E-Loyalty: Your Secret Weapon on the Web: Harvard Business Review, July-August 2000.

Retailresearch.org, (2014). Online Retailing Research - Centre for Retail Research, Nottingham UK. [online] Available at: http://www.retailresearch.org/onlineretailing.php [Accessed 24 Oct. 2014].

Rios, R. and Riquelme, H. (2008). Brand equity for online companies. Marketing Intelligence \& Planning, 26(7), pp.719--742.

Rojon, C. and Saunders, M. (2012). Formulating a convincing rationale for a research study. Coaching: An International Journal of Theory, Research and Practice, 5(1), pp.55--61.

Rouse, (2007). What is authentication? - Definition from WhatIs.com. [online] Searchsecurity.techtarget.com. Available at: http://searchsecurity.techtarget.com/definition/authentication

Rouse, M. (2006). What is PKI (public key infrastructure)? - Definition from WhatIs.com. [online] Searchsecurity.techtarget.com. Available at: http://searchsecurity.techtarget.com/definition/PKI [Accessed 28 Aug. 2014].

Rouse, M. (2008). What is nonrepudiation? - Definition from WhatIs.com. [online] Searchsecurity.techtarget.com. Available at: http://searchsecurity.techtarget.com/definition/nonrepudiation [Accessed 23 Aug. 2014].

Rouse, M. (2014). What is PKI (public key infrastructure)? - Definition from WhatIs.com. [online] Searchsecurity.techtarget.com. Available at: http://searchsecurity.techtarget.com/definition/PKI [Accessed 28 Aug. 2014].

Roztocki, N. (2001) "Using Internet-Based Surveys for Academic Research: Opportunities and Problems." Proceedings of the 2001 American Society of Engineering Management (ASEM) National Conference, Huntsville, AL, October 11-13, 2001, pp. 290-295.

Rubin, A. and Babbie, E. (1989). Research methods for social work. 1st ed. Belmont, Calif.: Wadsworth Pub. Co.

Salehnia, A. (2002). Ethical issues of information systems. Hershey, PA: IRM Press.

Selis, et al. (2002). Consumer privacy and data protection. [S.l.: s.n.

Sengupta, A., Mazumdar, C. and Barik, M. (2005). e-Commerce security—A life cycle approach. Sadhana, 30(2-3), pp.119--140.

Singh S (2014) Network Security Issues in e-Commerce; International Journal of Advanced Research in Computer Science and Software Engineering. Volume4, Issue3

Singh, M. and Waddell, D. (2004). E-business innovation and change management. Hershey, Pa.: Idea Group Pub.

Singh, S. and Diamond, S. (2012). Social media marketing for dummies. 1st ed. Hoboken, NJ: Wiley.

Smith, G. (2004). Control and security of E-commerce. Hoboken, N.J.: Wiley.

Software Engineering Institute, (2013). The CERT Division | SEI | CMU. [online] Cert.org. Available at: http://www.cert.org/ [Accessed 30 Aug. 2014].

Srinivasan, S., Anderson, R. and Ponnavolu, K. (2002). Customer loyalty in e-commerce: an exploration of its antecedents and consequences. Journal of retailing, 78(1), pp.41--50.

Successstories, (2014). Top 10 Deadliest Hackers of All Time. [online] Successstories.co.in. Available at: http://www.successstories.co.in/top-10-deadliest-hackers-of-all-time/ [Accessed 30 Aug. 2014].

Technopedia, (2003). What is a Script Kiddie? - Definition from Techopedia. [online] Techopedia.com. Available at:

http://www.techopedia.com/definition/4090/script-kiddie [Accessed 30 Aug. 2014].

Teoh, W., Chong, S., Lin, B. and Chua, J. (2013). Factors affecting consumers’ perception of electronic payment: an empirical analysis. Internet Research, 23(4), pp.465--485.

Turkish Civil Code, (2002). [online] Turkish Civil Code. Available at: http://www.tusev.org.tr/usrfiles/files/Turkish_Civil_Code.pdf [Accessed 1 Nov. 2014].

Udo, G. (2001). Privacy and security concerns as major barriers for e-commerce: a survey study. Information Management \& Computer Security, 9(4), pp.165--174.

Wildemuth, B. (2009). Applications of social research methods to questions in information and library science.1st ed. Westport, Conn.: Libraries Unlimited.

Yang, Q. (2003). [online] Giac.org. Available at: http://www.giac.org/paper/gsec/2776/operating-system-security-secure-operating-systems/104723 [Accessed 31 Aug. 2014].

Zhang, G. and Liu, Z. (2011). Effects of influential factors on consumer perceptions of uncertainty for online shopping. Nankai Business Review International, 2(2), pp.158--171.

Zhang, Y. (2000). Using the Internet for survey research: A case study. Journal of the American Society for Information Science, 51(1), pp.57--68.

7.0 APPENDIX

Survey - English

Online Shopping and Payments Survey.

* Required

1-) What is your age group? *

- 18-26
- 27-35
- 36-44
- 45-54
- 55 or older

2-) What is your gender? *

- Male
- Female

3-) Which device do you use for online shopping? *

- Computer
- Mobile
- Tablet
- Other:

4-) Please give rank to the concepts below. (1 per row.) *

(About online shopping)

	Very Important	Important	Moderately Important	Of Little Imporance	Unimportant
Privacy & Security					
Design of Website					
Variety of Payment Options					
Availability of Website					
Customer Base & Social Media					

5-) I completely trust major e-commerce sites such as Amazon and E-Bay. *

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

6-) My trust level about an online shopping site would affect my method of payment. *

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

7-) I would buy from a website that I do not trust if I cannot find the product/service I want to buy elsewhere. *

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

8-) Views or comments of other customers would affect my choice about online payment. *

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

9-) I believe paying with........................ is the most viable method. *

- ○ Credit Card
- ○ Debit Card
- ○ E-Wallet (Paypal etc)
- ○ Other: ____________

10-) I concern about my security while using an e-payment system. *

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

11-) I would only use an online payment system I used or heard it before *

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

12-) I find it difficult to learn and/or use E-Wallet payment method. *

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

13-) I concern about my privacy if I give too much information about myself. *

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

14-) A bad website design or bad interface would give me a bad impression about the website's security. *

	1	2	3	4	5	
Strongly Disagree	○	○	○	○	○	Strongly Agree

15-) How often do you read Privacy Policies and/or Terms and Conditions on websites before accepting them? *

- ○ Most of the time
- ○ Sometimes
- ○ Rarely
- ○ Never

Survey – Turkish

Online Alisveris ve Odeme Anketi (TR)

* Required

1-) Yaş Grubunuz? *

- 18-26
- 27-35
- 36-44
- 45-54
- 55 veya üstü

2-) Cinsiyetiniz? *

- Bay
- Bayan

3-) Online alışverişlerinizi hangi cihaz ile gerçekleştiriyorsunuz? *

Other(diğer)

- Bilgisayar
- Mobil
- Tablet
- Other:

4-) Asagidaki konseptleri online alisverislerinizi baz alarak onem bakimindan isaretleyiniz *

	Asiri Onemli	Cok Onemli	Onemli	Kismen Onemli	Onemsiz
Guvenlik & Kullanici Gizliligi					
Website Dizayni					
Odeme Yontemlerinin Cesitliligi					
Websitenin Ulasilabilirligi					
Musteri Tabani ve Sosyal Medya					

5-) Amazon, E-Bay gibi sitelere tamamen guvenirim *

	1	2	3	4	5	
Tamamen Katiliyorum	○	○	○	○	○	Kesinlikle Katilmiyorum

6-) Bir alisveris sitesine karsi duygudum guven seviyesi benim online odeme methodumu etkiler; *

	1	2	3	4	5	
Tamamen Katiliyorum	○	○	○	○	○	Kesinlikle Katilmiyorum

7-) Eger istedigim bir urun yada servisi guvendigim sitelerde bulamadiysam guvenmedigim bir siteden alirim. *

	1	2	3	4	5	
Tamamen Katiliyorum	○	○	○	○	○	Kesinlikle Katilmiyorum

8-) Baska musterilerin yorumlari ve gorusleri benim online odeme methodumu etkiler *

	1	2	3	4	5	
Tamamen Katiliyorum	○	○	○	○	○	Kesinlikle Katilmiyorum

9-) Bence .... ile odeme en iyi online odeme seklidir. *

- ○ Kredi Karti
- ○ Debit Karti (Banka Karti)
- ○ E-Cuzdan (PayPal vs)
- ○ Other:

10-) Online odeme yaparken guvenligim hakkinda endise duyarim *

	1	2	3	4	5	
Tamamen Katiliyorum	○	○	○	○	○	Kesinlikle Katilmiyorum

11-) Sadece daha onceden kullandigim veya duydugum bir odeme sekli ile odeme yaparim. *

	1	2	3	4	5	
Tamamen Katiliyorum	○	○	○	○	○	Kesinlikle Katilmiyorum

12-) E-Cuzdan ile odeme yapmayi yada ogrenmeyi zor birsey olarak goruyorum. *

	1	2	3	4	5	
Tamamen Katiliyorum	○	○	○	○	○	Kesinlikle Katilmiyorum

13-) Kendim hakkinda bir siteye fazla bilgi verirsem, gizliligim hakkinda endise duyarim. *

	1	2	3	4	5	
Tamamen Katiliyorum	○	○	○	○	○	Kesinlikle Katilmiyorum

14-) Kotu bir website dizayni bende o sitenin guvensiz oldugu izlenimini verir. *

	1	2	3	4	5	
Tamamen Katiliyorum	○	○	○	○	○	Kesinlikle Katilmiyorum

15-) Girdiginiz websitelerde gizlilik / kullanici sozlesmelerini ne kadar siklikla okursunuz? *

- ○ Cogu zaman
- ○ Bazen
- ○ Nadiren
- ○ Hic Okumam