Advances in Economics and Business Management (AEBM)
Print ISSN: 2394-1545; Online ISSN: 2394-1553; Volume 2, Number 10; April-June, 2015 pp. 1045-1048
© Krishi Sanskriti Publications
http://www.krishisanskriti.org/aebm.html

Ethical Problems of E-Retailing in India

Alamuri Megha Gupta[1] and Satish R. Billewar[2]

[1]JJT University, Jhunjhunu, Rajasthan, India
[2]Datta Meghe College of Engineering Navi Mumbai, India
E-mail: [1]megha.alamuri@gmail.com, [1]avg@armiet.com, [2]satish.billewar@gmail.com

Abstract—*The World Wide Web has changed the traditional way of business culture. So the businesses also started to change the way of perspectives. New concept creates new complexities. The need has arrived to examine the ethics in this new form of business which is known as E-Retailing. Businesses are efficiently implementing new policies and finding the opportunities. E-Retailing has increases the choices for the customers. Internet is providing so many advantages to the consumers for their daily needs. But on the other side, this new platform has created new challenge of unethical and social activities. E-Retailing is growing rapidly from last decade. The customers have started to rise the questions on various ethical and social issues. These problems has become the dark side of E-Retailing. Ethics is always a very complicated to decide right or wrong in any activity.*

Keywords*: E-Retailing, social, ethics, customer, Business*

1. INTRODUCTION

E-Retailing is the shopping method to do the retailing business electronically on the internet. The companies can advertise their products on the on the websites which performs the role of platform between companies and customers. The customers can choice the product and pay for it electronically. An internet is the backbone of the websites for the businesses. An internet itself is so vast that thousands of people around the world shares their information with the companies for their needs, especially for E-Retailing. E-Retailing provides the ability to do shopping securely where the net banking or credit cards perform through verification and validation of the data.

E-Retailing is one of the best platform for both the Companies and the customers. But this also gives access of the companies of personal data and all financial details of customer. The personal data and every small detail about the customer is the big asset for the companies. Now the time comes, where the companies has to decide whether they should use this information or not. If the companies are using it, they can sell variety of products to the customers and they will get big market also. But this is the fraud with the customer who have faith on company. The customer shares his data with the faith that the company has the responsibility to protect his data from all unauthorized access and offences because he is doing business with company. But what if the company itself is misusing it ?

2. OBJECTIVES OF STUDY

The main objective of the study is to find ethical and social problems in E-Retailing. The objective is –

- To study the ethical and social issues in E-Retailing
- To find threats to E-Retailing
- To give solutions to both the companies and customers of E-Retailing.

3. AN ETHICAL ISSUES OF E-RETAILING

At the early stages of internet, it was just considered as the platform to collect the information. Then from the emergence of retailing businesses, internet has been commercialized. Now, the banks have also started their business activities online. The involvement of money started treat to both the parties – companies and customers.

3.1 Web Spoofing

Web Spoofing is the fraud technique where the attacker creates a fake website very similar to original one. Like, attacker creates the website www. icicie.com which is very similar to the website of ICICI bank[2]. When the customer search the website on the google, this fraud website also becomes the option on search page. If the customer selects the option of this fraud website and do all transactions, the customer don’t notice it due to the similarity with the original website.

3.2 Cyber Squatting

Cyber Squatting is an activity where the attacker creates the websites just to infringe the trademark of one famous company. The purpose of these websites is to just extort the money from the original company. In 2000, BBC won the cyber squatting case against a firm which created the URL named bbcnews.com. In 2007, Dell also filed case against BelgiumDomains for cyber squatting[1].

3.3 Online Piracy

Online Piracy is an ethical activity where a person or a firm uses their software and hardware technologies to steal music, videos or e-books and sell it to unauthorized people. There are some software available on the internet which provides the facility to download the songs free of cost without the authorization of the user. Above to all, the creates the CD and DVD of songs and movies and sale in retail markets.

3.4 E-mail Spamming

E-mail Spamming is the type of fraud case where spammer sends the mails on the users mail id to get users financial information like credit card number or bank account details. Then the spammer forces the user to deposit some amount on certain account. In some cases, the spammer misdirect the user to the fake websites to fill up the personal information of the user. This is called as phishing[1].

3.5 Privacy Invasion

This is a one of the most important privacy issue. The company to which we have submitted our personal data share our personal data to other companies for their personal benefits. These company distribute the data of the customers based on gender, age, job and various other categories. This has also become the side business of these companies where they get certain amount against the data in quantity. Then the company which has purchased the data starts to send the advertisements on the mail id of the customers based on their personal interest.

3.6 Unauthorized Intruders

When the customer fill up the data for the registration, the unauthorized intruder may drain the personal data of the customer to his server[2]. Protecting the drainage of the data is the biggest challenge. An internet is a very complex media. Patching all the holes is technologically and economically can't possible. Finding unauthorized intruder is practically a very difficult task.

3.7 Malicious Programs for Cookies

Cookies are the special files created to store the repeated queries on the web. If the customer uses some websites or web pages repeatedly, then cookies saves the links in their files and saves time to repeatedly search the same server. The attackers creates the malicious programs with the intention steal very important data from the cookies like credit card numbers and passwords of the user.

4. THREATS IN E-RETAILING

E-Retailing has several security issues. Some of the important security issues are interception of the data, malicious programs, misdirection of the data and identification of true party in transaction. When an administrator need to secure E-Retailing sites, it is important to remember you are the part of the link system. The weak security is always associated with allowing attackers to get the access of personal information and misuse of it. Thus weak security becomes an ethical issue where an E-Retailing company need to pay more for customer security. But company don't take responsibility of security of customer data because they consider customer just an entity of the transaction process or business and customer faces the consequences of it.

4.1 Trojan Horses

A Trojan Horse is a set of malicious program which resides behind another good program and performs malicious activities. One of the best example is the Trojan Horses resides behind some best looking screen savers[3]. When we download the screen saver and install it, Trojan Horses don't create problem to screen or front look but it starts to damage the system internally. Generally Trojan Horses comes from the free software downloaded from internet. Nothing is free on internet. This is the fact where the customer need to be careful. This is to make sure that the customer should check authenticity of the software from confident sources.

4.2 Viruses and Worms

Viruses and worms are the most common threats on web. There are always confusion of the difference of these both concepts. Virus is the malicious program purposefully made to damage the system. Virus need a host program to spread it in maximum part of the system. It infects the host and cause the damage when user open this infected host file. The impact of the virus is depend on the type of host[3].

However, Worms are different than viruses. Worms don't need a host to create problem in the system. Indeed, these are the malicious programs which replicates itself on internet so fast that if it comes to user's computer, it hangs or stops user's system in very few hours. MS blaster worm is one of the best example which can shut down an E-Retailing server. It uses most of the valuable resources of the internet of E-Retailing server and stops most of the processing power.

4.3 Ping of Death Attack

When we send a mail or surf on internet, the data use to sent in the form of packets between two computers. These packets contains the information known as TCP/IP protocol[4]. These protocols allows to send the data of maximum 65,536 bytes from one computer to another. The Ping of Death Attack is the concept where attacker sends the packets of maximum size of 65,536 bytes on same TCP/IP by which memory buffer of the E-Retailing server overloaded. In some cases, the server causes crash.

4.4 Logic Bombs

This is one of the version of the Trojen Horse. This is very similar to time bomb. The logic of the attacks are very specific based on event or time. The logic bombs creates a malicious set of instructions or meaningless code after a particular event or specific time by which an application or processes on E-Retailing server get affected.

4.5 Service Attack

This is the type of attack where the attacker try to deny the services of the customers provided by the E-Retailing server. So sometimes it is also known as Denial of Service Attacks. Here the attackers goal is not to damage the files on the server, but he tries to send huge amount of useless data on the server[5]. As the server cannot process this huge information and the data starts to overflow. The ultimate result is, the server get confuse and automatically shut down.

4.6 SYN Flooding

When a user send a mail from his own computer to other, a set of messages exchanges between user computer and server, which is known as “Handshake”. In the initiation of this process, the user computer sends synchronization message (SYN) to server and server reply it by sending synchronization acknowledgment (SYN ACK) to user computer. To complete the internet connection, the user computer again send last acknowledgement (ACK) message and server wait to get it. This is considered as half opened connection where the attacker send malicious messages and overload the memory and processing power of server[4].

5. SOLUTIONS TO CUSTOMERS

Nowadays, internet has become a very risky platform for transactions. It is full of both facilities and threats. It customers are using internet, then should also know the precautionary measures[6].

5.1 Keep computer up-to-date

Customer should keep computer up-to-date by installing antivirus, updates and all resent versions. Make sure that the browser is also updated. Upgraded version of the software should have latest fixes and security patches. Also, windows operating system provides latest patches in updates to secure from viruses[7].

5.2 Don’t open unknown E-mails

Internet is a very friendly media where anybody can get E-mails of others. The attackers can send any malicious data through e-mails[8]. If user opens that message, there can be a chance to get infected by any one of the threat. The users need to take care of not to open any promotional or unknown messages. Make sure to mark on the provision in the setting to send these mails automatically in junk or spam folder[7].

5.3 Install security applications

The users should install an antivirus with real time protection. There are so many good anti- viruses are available like AVG, Norton, McAfee, Kaspersky, Avast and so on. Apart from that there are so many free antivirus tools like Microsoft Security Essential are available which keeps computer clean from spyware, adware, Trojan Horses, worms etc. There are some of the free tools like Windows Defender, S&D and Spybot which remove all hidden and stuck infections, which even can’t be detected by antivirus.

5.4 Be alert at the time of transactions

Sense everything at the time of browsing on web. Especially, the bank transactions are more attached to threat efforts. Don’t give personal details to any website unless and until the website it official and confident.

5.5 Use updated web browsers only

Due to the up gradations of the software, threats have also modified by the attackers. Thus, make sure to use the upgraded web browser also. Enhance the toolbars of the browsers also by which it helps to use the features of the browser easily and more efficiently[8].

5.6 Aware of authentication techniques

E-Retailing server designers use multilevel identification processes to authenticate the users and to perform safety transactions. The customer should be aware of these authentication techniques. These are very simple and common to multiple websites. If the customer gets any transaction without any authentication on main server, the website may be faked.

6. CONCLUSION

As the web is growing rapidly, the companies have also started to shift their businesses to this new platform which is known as E-Retailing. Businesses have brought money and also introduced their threats. The attackers have innovated various ways to collects customers personal information either to hazard them financially or to sell the information to other companies[9]. Internet is affecting lives positively as well as negatively than ever before. So when customer is getting benefits out of it, simultaneously he must have knowledge to secure himself from it’s threats.

REFERENCES

[1] Ebrahimi & Leprévost, F., Erard, R., 2000, “How to bypass the Wassenaar arrangement: a new application for watermarking” in *Proceedings of the 2000 ACM workshops on Multimedia*, Los Angeles, California, US. pp161-164

[2] Logan, PY. & Clarkson, A. (2005), “Teaching students to Hack” in *Proceedings of SIGCSE ’05, February 23-27*, St Louis, Missouri, USA

[3] JIBC Report, Journal of Internet Banking and Commerce, “Analyzing Perceived Risks and Website attributes in E-Retailing: A study from India”, August 2013, Vol 18, no.2

[4] Ford, W. 1994, “Standardizing Information Technology Security”, *StandardView*, vol. 2, issue 2, pp. 64-71

[5] eTechnology Group of IMRB(2004), “Consumer E-Retailing in India”, Internet and Mobile Association of India-IAMAI, pp 14-30

[6] IMRGWorld – a primary source in e-Business Intelligence prepared by Aadeening “, B2C Global E-Retailing Overview ,April 2012

[7] Aashit Shah and Parveen Nagree, “Legal Issues of E-Retailing”, Nishith Desai Associates.

[8] White, G.B., Cothren, C., Williams, D. & Davis, R.L. (2004), “*Principles of Computer Security. Security+ and Beyond”*, McGraw Hill, Illinois.

[9] IMRB Report, “Consumer E-Retailing in India “, May 2004