

Impact of Ethics in Electronic Commerce

Ashlin Nimo J R ^{1*}, Ganesh Kumar R ²

^{1,2} Assistant Professor, School of Management,
Vel Tech Rangarajan Dr Sagunthala R & D Institute of Science and Technology, Chennai
*Corresponding author E-mail: jrashlinnimo@gmail.com

Abstract

Internet was a tool to search information and communicate with each other during the early days of its emergence. Now, we can state that Internet has been commercialized (Electronic Commerce emerged). Nowadays, all businesses are taking place online. The online system gives a lot of merits to both customers and business organizations. But the demerits of electronic commerce are unavoidable. The major drawback of e-commerce is its ethical issue. These ethics issues are because of irresponsible parties who are a threat to both customers and business organizations. The online platform is not the same as traditional brick and mortar stores. Is it necessary to consider ethical issues in business? If so, whether steps should be taken to implement and address ethical issues.

Keywords: business ethics, electronic commerce, security, threats.

1. Introduction

Electronic commerce is the buying and selling of goods and services, or the transmitting of funds or data, over an electronic network, primarily the internet. Items can be promoted, distributed and payment can be made online. Because of the extent of online promotion, sites can be viewed by millions of customers who get up to date information about the products which match their demand for free of cost. The major merit of electronic commerce is the capability of giving secured shopping through the web. It provides immediate verification and validation of card transactions. This made the electronic commerce sites popular as it's cheaper than traditional form of selling.

1.1 What is Business Ethics?

Ethics or moral philosophy is a branch of philosophy that involves systematizing, defending and recommending concepts of right and wrong conduct. Ethical rules are the guidelines which explain how one person should behave with others. Business Ethics apply to all of us and are proposed to accomplish great outcomes for all individuals in all circumstances. A manager has to face lot of ethical questions while decision-making and this constitutes Business Ethics. The several choices chosen by managers while taking decisions are:

Social Contract Theory-All organizations have ethical responsibility to all sections of society.

Stakeholder theory-Managers are responsible to practice ethics while running a company towards stakeholders.

2. Objectives of Study

- The primary objective of the study is to arrive at the ethical issues related to electronic commerce.
- To find out the threats to users of Electronic Commerce.

- To learn better ways on how businesses and customers could be protected from online threats.

3. Ethics in e-commerce

Both political and social considerations in e-commerce businesses are supposed to be guided by ethics. The prime factors to be considered by an individual or an e-commerce organization are responsibility, accountability, liability and due process. Practising ethics is easy as we are reliable, we don't steal, and we do satisfy promises. Following ethics in organizations is easy as a result of the above mentioned details. If an organization is following ethics, it will be seen in the quality of the products and the way an organization treats its customers. Being deceitful, negligent and unskilled, a professional could be put into hazards. At certain moments, performing right things is a challenge. One must be bold enough to face challenges. Being successful and strong in online industry means a person admitting their mistakes and being careful next time. Earning reliability from customers is a tedious job as there won't be any direct communication with customers. If any entity wishes to succeed in the market and beat competition, they must practise ethics towards its customers.

4. The Ethical Issues in e-commerce

When web was developed, it helped only for searching and communication with each other. Now, it's been used for all purposes including banking transactions. Though it has several advantages it has a major drawback too i.e. Ethical Issues. So, before implementing any online processes or businesses one must be through with the online ethical issues and they must take precautionary steps to avoid complications out of it. The different online issues are:

1. Web spoofing:

Website spoofing involves websites which are created to steal sensitive information such as username and password. For example the attacker uses number 0 instead of using o in certain websites. Customers won't be aware of this and use such websites and perform their transactions.

2. Cyber Squatting:

Cyber-Squatting is the process of purchasing domain name by a cyber-squatter and he then sell that domain to the actual business person for greater price.

3. Privacy Invasion:

It occurs when the customers' information are provided to an unauthorized party. This occurs in the following ways:

Electronic business gathers information from customers in many ways like to view a webpage itself some sites ask us to register by using our basic information like age, contact number, our interests. The information collected may be sold to companies for huge traffic for their business. Safeguarding customer information is the most tedious part of online business.

Online piracy is the unauthorised copyright of intellectual properties such as e-books, music or videos.

4. Email Spamming:

Email spanning is forwarding unwanted contents to unauthorized customers through e-mail. Spammer is the people who spam their email. Spammers usually send email to get credit card and account information to defraud them.

5. Threats in Electronic Commerce

There are various threats in ecommerce. Some threats occur by chance and few are made purposefully. Few errors can also be due to the carelessness or inability of a human being, malicious code attacks, phishing, etc.

Security is also a major threat in e-commerce. If unauthorized users are able to access your information, it shows that your system is unsecured. Few people share information in public and if so is it necessary to safeguard their data in internet? Is it ethical when punishments to criminals who gather data over internet and to criminals who steal personally vary? Server is a very high capacity computer with a huge processing power and storage space with a special operating system.

1. Malicious Code Attacks:

Viruses and worms are the threats which everyone is aware of and it comes under this category of malicious code attacks. Both words may look identical and both are very different.

Virus is something which attaches itself in an executable code and it causes harm while executing code or opening a file. Virus requires a file and when it's executed it causes damage like deleting a file or formatting the entire contents.

Worm doesn't require a host to affect the system and it is different from virus.

Worm itself infects millions of computers globally in a fraction of seconds over internet. Example, MS Blaster Worm shutdown parts of internet and affected the performance of servers.

2. Denial of service attacks:

The ultimate purpose of this attack is to affect the services provided by the e-commerce servers to customers and because of this the server collapses. There won't be any wish to affect customers and their actual purpose is to shut down the server.

3. Ping of death:

The information which we want to communicate is converted to data packets and then it is shared over email or internet. Transmission Control Protocol/Internet Protocol (TCP/IP) is used to control the flow of data packets. Huge data packet is transmitted, which leads to server overloading and the memory buffers.

6. Implications of eCommerce

Web became a virtual eco-system for all businesses in the world. With the ease of searching and communicating information internet has emerged and now human life can't exist without internet. There are many issues in e-commerce like legal, moral, ethical, political and social issues.

7. Keep your computer safe from online threats

Internet is a combination of advantages and hazards. While using WWW there are chances of viruses to enter in your computer and get attached with a file and ultimately it causes harm to the entire system when it's executed. Precautionary measures have to be taken before using internet to avoid consequences.

1. Security Applications First:

You should install anti-virus software before using internet. There are many paid versions of anti-virus software like Kaspersky, Panda, Webrom, McAfee which are more secured and free versions of anti-virus softwares like AVG antivirus, Avast antivirus which provides security while viewing few websites. Also you require antispyware software which can scan your system to detect spyware, adware, Trojan horses, Worms, etc.

2. Start up to date:

You should update your OS, anti-virus software and web browsers regularly. Keep your OS and anti-virus software for automatic updating so that the software will be up-to-date and gets the maximum protection. Renew your anti-virus license regularly to get the updated version.

3. Don't open emails which are not known:

While using email in outlook, windows mail, Eudora, etc., don't open emails from unknown senders. Don't open the attachments of emails while you are accessing gmail, hotmail or yahoo mail.

4. Use the right web browser:

Use upgraded browsers like Google Chrome for surfing which alerts the users of unauthorized access or notifies the users of unauthorized sites through banner display.

5. Observe all things:

This is also called as phishing where you will be re-directed to another wrong site which collects your user name and password without your knowledge. This username and password information is used to commit crimes such as credit card theft and other crimes.

6. Authentication:

Due to security issues, e-commerce service providers have taken measures to screen out unauthorized access to their websites. The different authentication protocols are security questions, cryptography, biometrics, etc.

8. Conclusion

The internet is growing continuously and will go forever. There will come a time when software will be developed to see what a customer has seen, viewed and done using the internet. There will come a time when we won't be able to identify which website is real and which is fake. Security and privacy will be the major concern in the upcoming future too and many will attempt to do online fraud and the customers and businesses will become the victim of them. Applying good ethical standards in your business is a way to attract customers. Once the customers are dissatisfied with a particular part of your business, regaining them will be a tedious task. So, one has to concentrate more on ethical policies and practises. Ethics also affects sales, marketing, pricing and all parts of a business. So, it is good to follow ethical standards while setting up and running a business.

References

- [1] Conklin, W.A, White, G.B. Cothren C., Williams D. and Davis R.L., 2004, Principles of computer security, Security + and Beyond, McGraw Hill, Illinois
- [2] Ford W, 1994, Standardizing Information Technology Security, Standard view, Vol. 2, Issue.2, pp. 64-71
- [3] Narayana Rao, 2014, A deliberation of ethical concern in E-Commerce, Vol. 11, Issue.5
- [4] Gehling B. & Stankard D, 2005, E-Commerce Security in Information security curriculum development conference, 2005, pp. 3238, Kenneshaw, GA