ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 7, July 2013

The study of E-Commerce Security Issues and Solutions

Niranjanamurthy M [1], **DR. Dharmendra Chahar** [2]

Research Scholar, Dept. of MCA, MSRIT, Bangalore, INDIA[1]

HOD. Dept. of CS & IT, Seth G. B. Podar College, Nawalgarh (Jhunjhunu) -333042, INDIA[2]

Abstract: E-commerce Security is a part of the Information Security framework and is specifically applied to the components that affect e-commerce that include Computer Security, Data security and other wider realms of the Information Security framework. E-commerce security has its own particular nuances and is one of the highest visible security components that affect the end user through their daily payment interaction with business.
E-commerce security is the protection of e-commerce assets from unauthorized access, use, alteration, or destruction.
Dimensions of e-commerce security-Integrity, Non-repudiation, Authenticity, Confidentiality, Privacy, Availability. E-Commerce offers the banking industry great opportunity, but also creates a set of new risks and vulnerability such as security threats. Information security, therefore, is an essential management and technical requirement for any efficient and effective Payment transaction activities over the internet. Still, its definition is a complex Endeavour due to the constant technological and business change and requires a coordinated match of algorithm and technical solutions.
In this paper we discussed with Overview of E-commerce security, Understand the Online Shopping Steps to place an order, Purpose of Security in E-commerce, Different security issues in E-commerce, Secure online shopping guidelines.

Keywords: E-Commerce Security Issues, Security measures, Digital E-commerce cycle/Online Shopping, Security Threats, Secure online shopping guidelines.

I. INTRODUCTION

E-commerce Security is a part of the Information Security framework and is specifically applied to the components that affect e-commerce that include Computer Security, Data security and other wider realms of the Information Security framework. E-commerce security has its own particular nuances and is one of the highest visible security components that affect the end user through their daily payment interaction with business.

Today, privacy and security are a major concern for electronic technologies. M-commerce shares security concerns with other technologies in the field. Privacy concerns have been found, revealing a lack of trust in a variety of contexts, including commerce, electronic health records, e-recruitment technology and social networking, and this has directly influenced users.
Security is one of the principal and continuing concerns that restrict customers and organizations engaging with ecommerce.
Web e-commerce applications that handle payments (online banking, electronic transactions or using debit cards, credit cards, PayPal or other tokens) have more compliance issues, are at increased risk from being targeted than other websites and there are greater consequences if there is data loss or alteration. Online shopping through shopping websites having certain steps to buy a product with safe and secure.
The e-commerce industry is slowly addressing security issues on their internal networks. There are guidelines for securing systems and networks available for the ecommerce systems personnel to read and implement. Educating the consumer on security issues is still in the infancy stage but will prove to be the most critical element of the e-commerce security architecture. Trojan horse programs launched against client systems pose the greatest threat to e-commerce because they can bypass or subvert most of the authentication and authorization mechanisms used in an e-commerce transaction. These programs can be installed on a remote computer by the simplest of means: email attachments.
Privacy has become a major concern for consumers with the rise of identity theft and impersonation, and any concern for consumers must be treated as a major concern for e-Commerce providers.

II. RELATED WORKS

Security is one of the principal and continuing concerns that restrict customers and organizations engaging with

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 7, July 2013

ecommerce. The aim of this paper is to explore the perception of security in e-commerce B2C and C2C websites from both customer and organizational perspectives. [1]

With the rapid development of E-commerce, security issues are arising from people's attention. The security of the transaction is the core and key issues of the development of E-commerce. This paper about the security issues of E-commerce activities put forward solution strategy from two aspects that are technology and system, so as to improve the environment for the development of E-commerce and promote the further development of E-commerce. [2]

Web applications increasingly integrate third-party services. The integration introduces new security challenges due to the complexity for an application to coordinate its internal states with those of the component services and the web client across the Internet. [3]

Ecommerce web site owners on one side are thinking of how to attract more customers and how to make the visitors feel secured when working on the site, on the other side how the end users should rate a ecommerce website and what they should do to protect themselves as one among the online community. Our objective of writing this research analysis journal is to make the readers to have clarity of thoughts on the technology which helps all of us to do secure transactions along with safety tips. And how ecommerce site owners, have to make their online visitors to be of much comfort or Trust an ecommerce site via Trust marks, and by their security strategies. [4]

Each phase of E-commerce transaction has a security measures.

E-commerce Transaction Phases			
Information Phase	Negotiation Phase	Payment Phase	Delivery Phase
Security Measures			
Confidentiality Access Control Integrity Checks	Secure Contract Identification Digital Signatures	Encry-ption	Secure Delivery Integrity Checks

Fig.: Security measures in different phases of E-commerce Transaction. [5]

Viruses are a nuisance threat in the e-commerce world. They only disrupt e-commerce operations and should be classified as a Denial of Service (DoS) tool. The Trojan horse remote control programs and their commercial equivalents are the most serious threat to e-commerce. Trojan horse programs allow data integrity and fraud attacks to originate from a seemingly valid client system and can be extremely difficult to resolve. A hacker could initiate fraudulent orders from a victim system and the ecommerce server wouldn't know the order was fake or real. Password protection, encrypted client-server communication, public-private key encryption schemes are all negated by the simple fact that the Trojan horse program allows the hacker to see all clear-text before it gets encrypted. [6]

Due to the increase in warnings by the media from security and privacy breaches like identity theft and financial fraud, and the elevated awareness of online customers about the threats of performing transactions online, e-commerce has not been able to achieve its full potential. Many customers refuse to perform online transactions and relate that to the lack of trust or fear for their personal information. [7]

The traditional authentication mechanism is based on identity to provide security or access control methods; in addition, traditional encryption and authentication algorithm require high computing power of computer equipment. Therefore, how to improve the authentication mechanism and optimize the traditional encryption and authentication algorithm may be the focus of P2P e-commerce. [8]

E-Commerce offers the banking industry great opportunity, but also creates a set of new risks and vulnerability such as security threats. Information security, therefore, is an essential management and technical requirement for any efficient and effective Payment transaction activities over the internet. Still, its definition is a complex endeavor due to the constant technological and business change and requires a coordinated match of algorithm and technical solutions. [9]

The success or failure of an e-commerce operation hinges on myriad factors, including but not limited to the business model, the team, the customers, the investors, the product, and the security of data transmissions and storage. Data security has taken on heightened importance since a series of high-profile "cracker" attacks have humbled popular Web sites, resulted in the impersonation of Microsoft employees for the purposes of digital certification, and the misuse of credit card numbers of customers at business-to-consumer e-commerce destinations. [10]

The analysis of G2C based online payment systems triggered conclusions which led to emphasize research on the security aspect on online payment systems. It was found that the credit card based payment systems

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 7, July 2013

were the most widely used means of conducting online payments. It was also extracted from the study that users want more simplified, convenient and secure online payment systems. [11]. The effect of security, protection and trust towards consumers as well as attitudes plays a key role in ecommerce implementation however, if well implemented, instantaneous flow of goods and services internally and externally. Besides, vital information could also be simultaneously processed to matched with data flowing from external ecommerce transactions which could allows for efficient and effective integration into organizational processes. [12]

Transactions between buyers and sellers in e-commerce includes requests for information, quotation of prices, placement of orders and payment, and after sales services. The high degree of confidence needed in the authenticity, confidentiality, and timely delivery of such transactions can be difficult to maintain where they are exchanged over the Internet. [13]

Privacy and security can be viewed as ethical questions. At the same time the privacy and security area attracts a large amount of attention from the commercial sector because it has the potential to determine the success or failure of many business ventures, most obviously e-commerce activities.[14]

Clearly, the online transaction requires consumers to disclose a large amount of sensitive personal information to the vendor, placing themselves at significant risk. Understanding (indeed, even precisely defining) consumer trust is essential for the continuing development of e-commerce.[15]

In online shopping online electronic payment function is the key issue to ensure the consumers are fast and convenient, we have to ensure the safety and secrecy of the parties to a transaction, which requires a complete electronic trading systems. [16]

III. PURPOSE OF STUDY

* Study the Overview of E-commerce security.
* Understand the Online Shopping - Steps to place an order.
* Understand the purpose of Security in E-commerce.
* Discuss the different security issues in E-commerce.
* Understand the Secure online shopping guidelines.

IV. DIGITAL E-COMMERCE CYCLE

Security is very important in online shopping sites.

Now days, a huge amount is being purchased on the internet, because it's easier and more convenient. Almost anything can be bought such as music, toys clothing, cars, food and even porn. Even though some of these purchases are illegal we will be focusing on all the item's you can buy legally on the internet. Some of the popular websites are eBay, iTunes, Amazon, HMV, Mercantila, dell, Best Buy and much more.

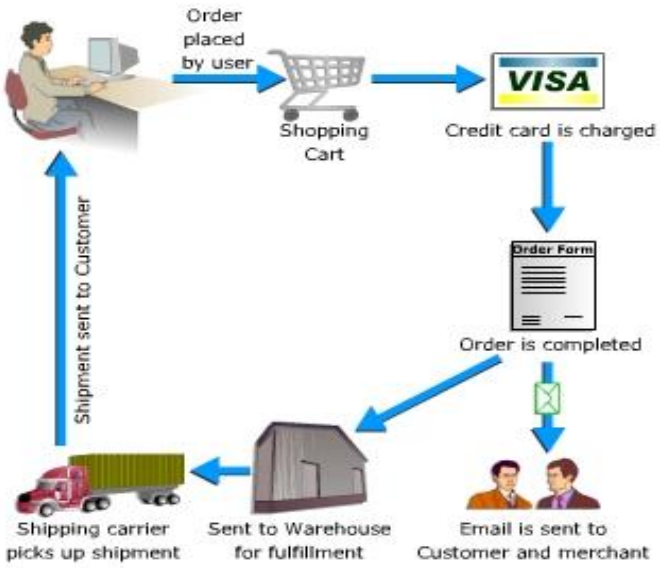

Fig1.: Digital E-commerce cycle

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 7, July 2013

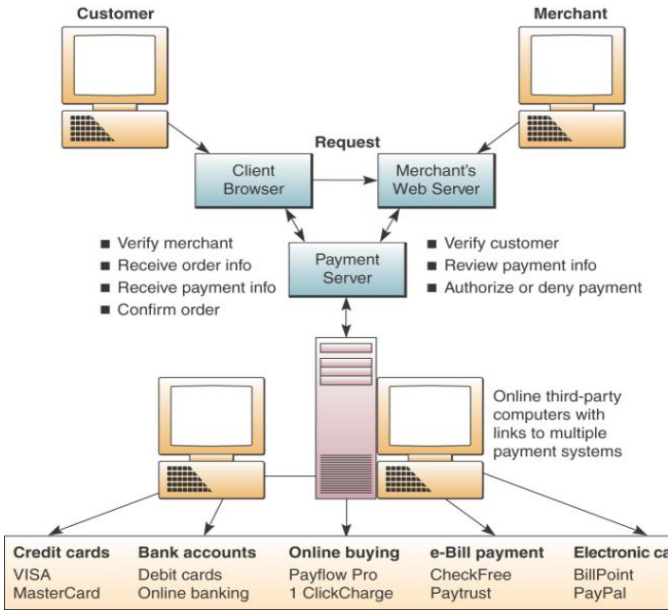

Fig2.: Digital E-commerce cycle

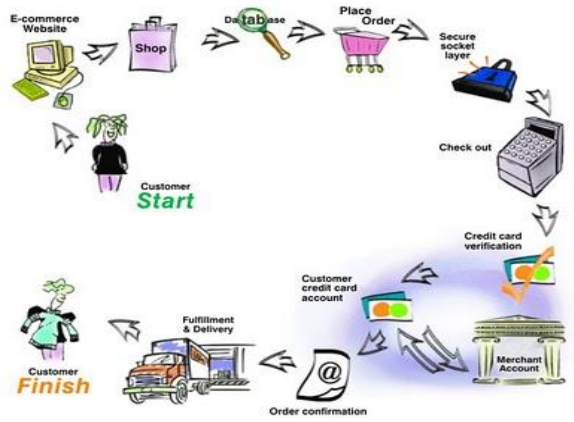

Fig.: Online Shopping - Steps to place an order

Resource: http://onlineshoppingproducts.blogspot.in/2010/10/online-shopping-steps-to-place-order.html

V. E-COMMERCE SECURITY TOOLS

- Firewalls – Software and Hardware
- Public Key infrastructure
- Encryption software
- Digital certificates
- Digital Signatures
- Biometrics – retinal scan, fingerprints, voice etc
- Passwords
- Locks and bars – network operations centers

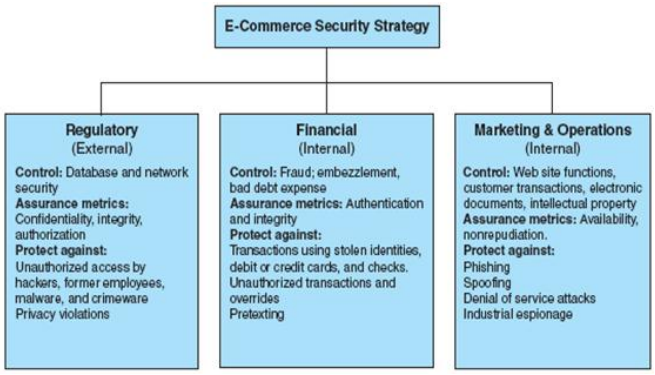

Fig:. E-Commerce Security Strategy

VI. PURPOSE OF SECURITY

1. Data Confidentiality – is provided by encryption / decryption.
2. Authentication and Identification – ensuring that someone is who he or she claims to be is implemented with digital signatures.
3. Access Control – governs what resources a user may access on the system. Uses valid IDs and passwords.
4. Data Integrity – ensures info has not been tampered with. Is implemented by message digest or hashing.
5. Non-repudiation – not to deny a sale or purchase Implemented with digital signatures.

__ Plaintext/Cleartext – message humans can read.

__ Ciphertext – unreadable to humans, uses encryption. Reverse process is call decryption.

__ A cryptographic algorithm is called a cipher. It is a mathematical function. Most attacks are focused on finding the "key".

VII. SECURITY ISSUES

E-commerce security is the protection of e-commerce assets from unauthorized access, use, alteration, or destruction. While security features do not guarantee a secure system, they are necessary to build a secure system.

Security features have four categories:

- Authentication: Verifies who you say you are. It enforces that you are the only one allowed to logon to your Internet banking account.
- Authorization: Allows only you to manipulate your resources in specific ways. This prevents you from increasing the balance of your account or deleting a bill.
- Encryption: Deals with information hiding. It ensures you cannot spy on others during Internet

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 7, July 2013

banking transactions.

- Auditing: Keeps a record of operations. Merchants use auditing to prove that you bought a specific merchandise.
- Integrity: prevention against unauthorized data modification
- Nonrepudiation: prevention against any one party from reneging on an agreement after the fact
- Availability: prevention against data delays or removal.

VIII. SECURITY THREATS

•Three types of security threats
–*denial of service,*
–*unauthorized access, and*
–*theft and fraud*

Security (DOS): Denial of Service (DOS)
•Two primary types of DOS attacks: spamming and viruses
•Spamming
–Sending unsolicited commercial emails to individuals
–E-mail bombing caused by a hacker targeting one computer or network, and sending thousands of email messages to it.
–Surfing involves hackers placing software agents onto a third-party system and setting it off to send requests to an intended target.
–DDOS (distributed denial of service attacks) involves hackers placing software agents onto a number of third-party systems and setting them off to simultaneously send requests to an intended target
•Viruses: self-replicating computer programs designed to perform unwanted events.
•Worms: special viruses that spread using direct Internet connections.
•Trojan Horses: disguised as legitimate software and trick users into running the program

Security (unauthorized access)
•Illegal access to systems, applications or data
•Passive unauthorized access –listening to communications channel for finding secrets.
–May use content for damaging purposes
•Active unauthorized access
–Modifying system or data
–Message stream modification
•Changes intent of messages, e.g., to abort or delay a negotiation on a contract
•Masquerading or spoofing –sending a message that appears to be from someone else.
–Impersonating another user at the "name"(changing the "From"field) or IP levels (changing the source and/or destination IP address of packets in the network)
•Sniffers–software that illegally access data traversing across the network.
•Software and operating systems' security holes

Security (theft and fraud)
•Data theft already discussed under the unauthorized access section
•Fraud occurs when the stolen data is used or modified.
•Theft of software via illegal copying from company's servers.
•Theft of hardware, specifically laptops.

IX. SECURE ONLINE SHOPPING GUIDELINES

1. Shop at Secure Web Sites
How can you tell if a Web site is secure? Secure sites use encryption technology to transfer information from your computer to the online merchant's computer. Encryption scrambles the information you send, such as your credit card number, in order to prevent computer hackers from obtaining it en route. The only people who can unscramble the code are those with legitimate access privileges. Here's how you can tell when you are dealing with a secure site:

- If you look at the top of your screen where the Web site address is displayed (the "address bar"), you should see https://. The "s" that is displayed after "http" indicates that Web site is secure. Often, you do not see the "s" until you actually move to the order page on the Web site.
- Another way to determine if a Web site is secure is to look for a closed padlock displayed on the address bar of your screen. If that lock is open, you should assume it is not a secure site.

Of course, transmitting your data over secure channels is of little value to you if the merchant stores the data unscrambled. You should try to find out if the merchant stores the data in encrypted form. If a hacker is able to intrude, it cannot obtain your credit data and other personal information. Be sure to read the merchant's privacy and security policies to learn how it safeguards your personal data on its computers. (See tip 3 below.)

2. Research the Web Site before You Order
Do business with companies you already know. If the company is unfamiliar, do your homework before buying their products. If you decide to buy something from an unknown company, start out with an inexpensive order to learn if the company is trustworthy.
Reliable companies should advertise their physical business address and at least one phone number, either customer

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 7, July 2013

service or an order line. Call the phone number and ask questions to determine if the business is legitimate. Even if you call after hours, many companies have a "live" answering service, especially if they don't want to miss orders. Ask how the merchant handles returned merchandise and complaints. Find out if it offers full refunds or only store credits.

You can also research a company through the Better Business Bureau (see listing below), or a government consumer protection agency like the district attorney's office or the Attorney General. Perhaps friends or family members who live in the city listed can verify the validity of the company. Remember, anyone can create a Web site.

3. Read the Web Site's Privacy and Security Policies

Every reputable online Web site offers information about how it processes your order. It is usually listed in the section entitled "Privacy Policy." You can find out if the merchant intends to share your information with a third party or affiliate company. Do they require these companies to refrain from marketing to their customers? If not, you can expect to receive "spam" (unsolicited email) and even mail or phone solicitations from these companies.

You can also learn what type of information is gathered by the Web site, and how it is — or is not — shared with others. The online merchant's data security practices are also often explained in the Privacy Policy, or perhaps a separate Security Policy.

Look for online merchants who are members of a seal-of-approval program that sets voluntary guidelines for privacy-related practices, such as TRUSTe (www.truste.org), Verisign (www.verisign.com), or BBBonline (www.bbbonline.org).

However, be aware that a strong privacy policy and membership in a Web-seal program don't guarantee that the Web merchant will protect your privacy forever. Policies can change. The company can file for bankruptcy and sell its customer data base. The Web merchant might be purchased by another company with a weaker privacy policy. And the company's data can be subpoenaed for law enforcement investigations or civil cases. You have little control over the use of your customer data in such matters.

Given all of these uncertainties, you will want to think about the sensitivity of the data that is being compiled about you when you shop online. We cannot prescribe the best approach to take. Each consumer has a different interpretation of what is considered "sensitive."

4. Be Aware of Cookies and Behavioural Marketing

Online merchants as well as other sites watch our shopping and surfing habits by using "cookies," an online tracking system that attaches pieces of code to our Internet browsers to track which sites we visit as we search the Web.

"Persistent" cookies remain stored on your computer while "session" cookies expire when you turn the browser off. Online merchants use cookies to recognize you and speed up the shopping process the next time you visit. You may be able to set your browser to disable or refuse cookies but the tradeoff may limit the functions you can perform online, and possibly prevent you from ordering online. Generally, you will need to enable session cookies to place an order.

Privacy advocates worry that as more and more data is compiled about us — without our knowledge or active consent — it will be combined to reveal a detailed profile, even our actual identities. This data is often collected to market goods and services to us, encouraging us to buy them. There are a number of companies that specialize in targeted online advertising called "behavioral marketing." Companies say consumers benefit by being exposed to more targeted advertising and that online merchants can make more money more efficiently by targeting the right shoppers. For example, you might buy a book on golf from Amazon, visit the Professional Golfer's Association site, purchase golf shoes at Zappos, and search online for golf courses near your home. When you do, a cookie or your computer's Internet Protocol (IP) address could be used to generate golf-related ads. When you open the USA Today site to read the morning news, you may see an ad offering you a new set of clubs at a discount. When you go back to Amazon later that day you might be offered a biography of Tiger Woods. What if your behavioral marketing profile is shared with others, without your permission? You might not care if a drug company shares your prescription drug information with a coupon service to save you money. But what if that same information were obtained by your employer, resulting in more expensive health insurance coverage?

5. What's Safest: Credit Cards, Debit Cards, Cash, or Checks?

The safest way to shop on the Internet is with a *credit card*. In the event something goes wrong, you are protected under the federal Fair Credit Billing Act. You have the right to dispute charges on your credit card, and you can withhold payments during a creditor investigation. When it has been determined that your credit was used without authorization, you are only responsible for the first $50 in charges. You are rarely asked to pay this charge. For more information on credit card consumer protections, see http://www.privacyrights.org/fs/fs32-paperplastic.htm#3

Make sure your credit card is a true credit card and not a debit card, a check card, or an ATM card. As with checks, a debit card exposes your bank account to thieves. Your checking account could be wiped out in minutes. Further,

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 7, July 2013

debit and ATM cards are not protected by federal law to the extent that credit cards are.

The "Restore Online Shoppers' Confidence Act" (P.L. 111-345) (signed December 29, 2010) makes it illegal for a company that sells goods or services online to give a consumer's credit card number (or other financial account number) to a third-party for sales purposes. This practice is known as "data passing." The Act prohibits a third-party seller from charging a consumer for any good or service, unless the seller (1) clearly and conspicuously discloses the material offer terms and that the third-party seller is not affiliated with the initial merchant and (2) receives express consent for the charge from the consumer. The third-party seller must obtain the full financial account number directly from the consumer. The initial online seller may not transfer a consumer's financial account number to a third-party seller. The Act also regulates "negative option" plans. A consumer must give express, informed consent before being charged for goods or services sold online through "negative option" marketing, such as "free trials" that the consumer must cancel in order to avoid being charged. Companies that use negative option plans must (1) clearly and conspicuously disclose the material terms of the transaction before obtaining the consumer's billing information, (2) obtain a consumer's express consent before charging the consumer, and (3) provide a simple mechanism to stop any recurring charges.

Online shopping by *check* leaves you vulnerable to bank fraud. And sending a cashier's check or money order doesn't give you any protection if you have problems with the purchase.

Never pay for online purchases by using a *money transfer service*. You could be transferring cash to a fraudster. Scammers will ask consumers to send them payment using a money transfer service such as Western Union or MoneyGram because they can get your cash fast and it's difficult to trace. Legitimate sellers normally do not ask consumers to send payment that way. Money transfer services should only be used to send money to people that you know well, not to unknown sellers of merchandise online. Watch the Consumer Federation of America's video about this at http://www.youtube.com/watch?v=R2ylW85g1So.

6. *Never Give Out Your Social Security Number*

Providing your Social Security number is not a requirement for placing an order at an online shopping site. There is no need for the merchant to ask for it. Giving out your Social Security number could lead to having your identity stolen. (See PRC Fact Sheet 17a, "Identity Theft: What to Do if It Happens to You," www.privacyrights.org/fs/fs17a.htm.)

7. *Disclose Only the Bare Facts When You Order*

When placing an order, there is certain information that you must provide to the web merchant such as your name and address. Often, a merchant will try to obtain more information about you. They may ask questions about your leisure lifestyle or annual income. This information is used to target you for marketing purposes. It can lead to "spam" or even direct mail and telephone solicitations.

Don't answer any question you feel is not required to process your order. Often, the web site will mark which questions need to be answered with an asterisk (*). Should a company require information you are not comfortable sharing, leave the site and find a different company for the product you seek.

8. *Keep Your Password Private*

Many online shopping sites require the shopper to log-in before placing or viewing an order. The shopper is usually required to provide a username and a password. Never reveal your password to anyone. When selecting a password, do not use commonly known information, such as your birthdate, mother's maiden name, or numbers from your driver's license or Social Security number. Do not reuse the same password for other sites, particularly sites associated with sensitive information. The best password has at least eight characters and includes numbers and letters. Read our Alert "10 Rules for Creating a Hacker Resistant Password" to help you choose a safer password.

9. *Check the Web Site Address*

The address bar at the top of your device's screen contains the web site address (also called the URL, or Uniform Resource Locator). By checking that address, you can make sure that you are dealing with the correct company.

Don't click on any link embedded within a potentially suspicious email. Instead, start a new Internet session by typing in the link's URL into the address bar and pressing "Enter" to be sure you are directed to a legitimate Web site.

10. *Don't Fall for "Phishing" Messages*

Identity thieves send massive numbers of emails to Internet users that ask them to update the account information for their banks, credit cards, online payment service, or popular shopping sites. The email may state that your account information has expired, been compromised or lost and that you need to immediately resend it to the company.

Some emails sent as part of such "phishing" expeditions often contain links to official-looking Web pages. Other times the emails ask the consumer to download and submit an electronic form.

Remember, legitimate businesses don't ask for sensitive information via email. Don't respond to any request for financial information that comes to you in an email. Again, don't click on any link embedded within a suspicious email,

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 7, July 2013

and always call the retailer or financial institution to verify your account status before divulging any information. For more information on phishing, visit www.antiphishing.org, and www.onguardonline.gov.

11. Always Print or Save Copies of Your Orders

After placing an order online, you should receive a confirmation page that reviews your entire order. It should include the costs of the order, your customer information, product information, and the confirmation number.

We recommend you print out or save a copy of the Web page(s) describing the item you ordered as well as the page showing company name, postal address, phone number, and legal terms, including return policy. Keep it for your own records for at least the period covered by the return/warranty policy.

Often you will also receive a confirmation message that is e-mailed to you by the merchant. Be sure to save and/or print this message as well as any other e-mail correspondence with the company.

12. Shop with Companies Located in the United States

When you shop within the U.S., you are protected by state and federal consumer laws. You might not get the same protection if you place an order with a company located in another country.

13. Pay Attention to Shipping Facts

Under the law, a company must ship your order within the time stated in its ad. If no time frame is stated, the merchant must ship the product in 30 days or give you an "Option Notice." This gives you an opportunity to cancel the order and receive a prompt refund, or agree to the delay.

Here are key shipping questions to ask:

- Does the site tell you if there are geographic or other restrictions for delivery?
- Are there choices for shipping?
- Who pays the shipping cost?
- What does the site say about shipping insurance?
- What are the shipping and handling fees, and are they reasonable?

14. Learn the Merchant's Cancellation, Return and Complaint-Handling Policies

Even under the best of circumstances, shoppers sometimes need to return merchandise. Check the Web site for cancellation and return policies. Be sure to check for the following:

- Who pays for shipping?
- Is there a time limit or other restrictions to the return or cancellation?
- Is there a restocking charge if you need to cancel or return the order?
- Do you get a store credit, or will the company fully refund your charges to your credit card? If the merchant only offers store credits, find out the time restriction for using this credit
- Does the merchant post a phone number and/or e-mail address for complaints?
- How long has the company been in business?
- Will they still be around when you need them?
- Is there an easy, local way for you to get repairs or service?
- Is there a warranty on the product, and who honors that guarantee?
- What are the limits, and under what circumstances can you exercise your warranty rights?

Don't expect less customer service just because a company operates over the Internet. This is especially important if you are buying something that may need to be cleaned or serviced on occasion.

15. Use Shopper's Intuition

Look at the site with a critical eye. And heed the old adage, "If it looks too good to be true, it probably is." If any of these questions trigger a warning bell in your head, you will be wise to find another online merchant:

- Are there extraordinary claims that you question?
- Do the company's prices seem unusually low?
- Does it look like the merchant is an amateur?
- Are there a lot of spelling or grammar errors?
- Does the company's phone go unanswered.
- The use of a post office box might not send up a red flag, but a merchant who does not also provide the company's physical address might be cause for concern.

16. Be Wary of Identity Theft

As online shopping becomes more common, there will be more cases of identity theft committed over the Internet. Imposters are likely to obtain their victims' identifying information using low-tech means like dumpster diving, mail theft, or workplace access to SSNs. But they are increasingly using the Web to apply for new credit cards and to purchase goods and services in their victims' names.

The same advice for avoiding low-tech identity theft applies to shopping on the Internet. Many are mentioned in the above tips. Most important: Be aware of who you are buying from. And use *true* credit cards for purchases, not debit cards.

We recommend that you check your credit card bills carefully for several months after purchasing on the Internet. Look for purchases you did not make. If you find some, immediately contact the credit card company and file a dispute claim.

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 7, July 2013

Order your credit reports at least once a year and check for accounts that have been opened without your permission. (See PRC Fact Sheet 17a , "Identity Theft: What to Do if It Happens to You," www.privacyrights.org/fs/fs17a.htm.)

17. Consider Using Single-use Card Numbers

Consumers using some brands of credit cards can get "virtual credit cards," or single-use card numbers, that can be used at an online store. Virtual credit cards use a randomly generated substitute account number in place of your actual credit card number. They can also be used to buy goods and services over the phone and through the mail but can't be used for in-store purchases that require a traditional plastic card.

With this free service, you never need to give out your real credit card number online. Among the card companies offering it are Citibank and Bank of America. Citibank calls their virtual credit card offering a Virtual Account Number while Bank of America calls it ShopSafe. You can configure the expiration date and the maximum amount allowed for a virtual credit card. card. Once used, the card is tied to the merchant where it was used, and cannot be used elsewhere.

18. Be Cautious with Electronic Signatures

A federal law enables shoppers to verify online purchases with merchants using an electronic signature. Usually, this process is nothing more than clicking on a box that says you accept the terms of the order.

The Electronic Signatures in Global and National Commerce Act, also known as the E-Sign Act, is a complex law. It states that electronic signatures and electronic records used in interstate and foreign commerce will not be denied validity just because they are in electronic form. Further, the law says that online purchases do not need to be accompanied by the more traditional handwritten signature on a paper document.

Consumer advocates opposed the law because it lacks important safeguard against fraud. For example, the law does not require online merchants to comply with such standards as message integrity (security and accuracy in transmission), privacy of customer data, and authentication of sender.

The faults of the E-Sign Act require you to shop cautiously on the Internet. The tips offered in this guide will help you make sure the online companies you choose are secure and honest.

19. Know How Online Auctions Operate

Online auctions connect buyers and sellers, allowing them to communicate in a bidding process over items for sale. Many people are drawn to online auction sites because they allow you to buy items at discounted prices. And they offer a chance to sell some of your unneeded or unwanted possessions to raise extra money. For the most part, online auction sites are a safe way to exchange goods. But it makes sense to be cautious and aware.

The first step in safely using an online auction site is to read the terms of use, which will outline key issues such as whether or not the seller or the site is responsible for any problems that arise. Learn a site's return policy, as it may be difficult to return merchandise bought at auction. It's critical to check the policy, because you may be required to follow the seller's refund policy, rather than that of the auction site.

Once a consumer has agreed to a price with a seller, the buyer and seller arrange for payment and delivery of the product. Successful bidders can usually choose among several payment options, such as credit card, online payment service, debit card, personal check, cashier's check, money order, or escrow service.

If a seller requests payment in cash by private courier, or by check or money order through an overnight delivery service, you have a right to be suspicious. This could signal an attempt to commit fraud by taking your money without delivering the merchandise.

It always makes sense to pay by credit card because you'll have an option to seek a credit from the credit card issuer (also known as a "chargeback") if the product isn't delivered or isn't what you ordered. For more information on credit card consumer protections see www.privacyrights.org/fs/fs32-paperplastic.htm#3

To protect both buyers and sellers, some auction sites prohibit the use of wire transfers as a payment method. The Federal Trade Commission recommends that buyers do not pay by wire transfer because if something goes wrong, you are left with no refund and no recourse.

Another popular way to pay at auctions is with online payment services, such as PayPal. In this scenario, the buyer and seller set up accounts that allow them to make or accept payments. Buyers provide payment information, like bank account or credit card numbers, and sellers give information about where payments should be deposited. Some online payment services offer protection if the seller doesn't ship the goods.

Sellers can be scammed too. Fake check scams are the most common problem, although they can be avoided by not accepting checks, especially cashier's or certified checks, as payment, and by waiting to ship the goods until you get your payment in a reliable form.

If a buyer offers you a cashier's (or certified) check for more than the amount of the item, and asks you to wire them the excess amount, don't do it. This it is a classic example of a fake check scam.

If you encounter a problem with a buyer or seller at an online auction site, such as eBay, it's important to report the problem to the site right away. You are probably not the only person being taken advantage of and you could help shut down illegal or unethical sellers by alerting the site to the problem. For more information on online auctions, see

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 7, July 2013

www.consumer-action.org/news/articles/internet_commerce_issue_spring_2008/#Topic_07

20. Understand Your Responsibility for Sales and Use Taxes Online

Generally Internet shopping is sales tax free, but there's a catch. If an online merchant has a physical presence in your state, it is required to charge you sales tax. In most states, consumers are required to pay tax on online purchases, even if the store doesn't collect it. Most states call this a "use tax." Efforts are underway to simplify the sales tax issue in many states.

21. Be Aware of Dynamic Pricing

Some online retailers use dynamic pricing to engage in price discrimination by charging different prices to different consumers for identical goods or services. When you purchase goods or services online, you may be paying a higher or lower price than another online customer buying the same item from the same site at the same time. While online shopping enables consumers to easily compare prices, it also allows businesses to collect detailed information about a customer's purchasing history and preferences. Online stores can use that information to customize the prices they charge you.

Amazon.com began experimenting with dynamic pricing in 2000. Different customers were offered different prices for the same product. Depending upon a consumer's purchase history and other information, Amazon might offer different prices matched to a customer's perceived willingness to pay a higher or lower price than the standard price.

In 2005, the University of Pennsylvania's Annenberg Public Policy Center published "Open to Exploitation: American Shoppers Online and Offline" (http://www.annenbergpublicpolicycenter.org/Downloads/Information_And_Society/Turow_APPC_Report_WEB_FINAL.pdf) The Annenberg study documented how most consumers who use the Internet are unaware how vulnerable they are to abuse by marketers and how the information that they provide can be used to exploit them. Researchers conducted a survey and found that about 2/3 of those surveyed did not know that it is legal "for an online store to charge different people different prices at the same time of day." The study also identified instances of dynamic pricing online. For example, one photography site charged different prices for the same camera depending upon whether online shoppers had previously visited a price-comparison site.

In 2010, the Wall Street Journal reported on a company that helps a major credit card issuer determine what deals to offer customers when they visit the issuer's site. The offer changed based upon information gleaned from the user's computer, rather than their credit-rating or other information provided by the customer. More recently, the same bank was reported to offer different car loan rates to users using different browsers. (http://consumerist.com/2010/11/01/capital-one-made-me-different-loan-offers-depending-on-which-browser-i-used/).

While dynamic pricing has existed for a long time for time-sensitive products such as airline tickets, hotel room reservations, and rental cars, it's difficult to justify the use of dynamic pricing for goods and services that are not of a time-sensitive nature.

Online merchants can easily implement dynamic pricing by placing cookies on a customer's computer which will track the user's past interactions with the site. By using this information, sites can customize their interactions based on your past activities. Online stores can read the cookies on your browser to determine what products or services you searched for and bought and how much you paid for them. This information helps them to predict how much you might be willing to pay for a product or service. In addition, click-stream technology allows a site to trace the path that a user follows as they view different pages on the site.

Some online stores may also consider other factors when determining pricing. For example, merchants might charge higher prices to customers who make repeated returns or demand extra service.

There are several ways that you may be able to defeat dynamic pricing. Obviously, do not log in to a site before you obtain a price quote. Be sure to clear the cookies from your browser before you visit a site. Visit sites from different browsers (Internet Explorer, Firefox, and others). Utilize price comparison sites that check prices from multiple vendors. Finally, if you do log in to a site, try leaving items in your shopping cart for a few days, to see if the merchant offers any discounts.

23. Additional Resources

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 7, July 2013

Listed below are Web sites that provide additional information about shopping online.

www.bbb.org and www.bbbonline.org	The Better Business Bureau certifies web merchants with a privacy seal of approval. You can research merchants through the BBB and also report e-commerce fraud problems at these sites.
www.fda.gov/ForConsumers /ProtectYourself/default.htm	Created by the U.S. Food and Drug Administration to provide shopping tips for buying online prescriptions and over-the-counter drugs on the web.
http://www.ftc.gov/bcp/menus /consumer/tech/online.shtm	The Federal Trade Commission guides for online shopping and E-payments.
http://www.ftc.gov/bcp/menus /consumer/tech/scams.shtm	The Federal Trade Commission's tips on Internet auctions.
www.ic3.gov	The FBI's Internet Fraud Complaint Center allows you to report suspected cases of Internet and e-commerce fraud.
www.lookstoogoodtobetrue.com	Federal law enforcement and industry task force helps prevent consumers from becoming victims of an Internet fraud schemes.
www.onguardonline.gov	FTC, other federal agencies, and the technology industry offer advice on identity theft, phishing, spyware, spam, online shopping and more.
www.safeshopping.org	Online shopping tips provided by the American Bar Association.

(Resource: https://www.privacyrights.org/fs/fs23-shopping.htm#4)

Small list of ways to protect you:

· Change your passwords from time to time
· Don't keep your sensitive or protected files in folders that have a revealing name
· Choose passwords with numbers, upper and lower case, 8 digitals long, and have special characters (!*&)
· Don't choose a password that you use anywhere else
· Get regular audits (www.comodo.com) – these services usually come with an icon that you can put on your store, and they have been known to boost sales
· Apply updates to your shopping cart when available
· Apply security patches to your shopping cart when available
· Always use https when navigating through your admin area (if you have SSL installed on your server)
· If you want (and have the option), consider deleting all customer credit card details after purchases
· Sign up with a managed firewall service (www.able-Commerce.com) – these services usually come with an icon that you can put in your store, and they have been known to boost sales. They are not free though
· Choose a shopping cart that records IP in the admin and store section.
· Choose a shopping cart that can blacklist (block) IP addresses and users

Remember that usually it's only the bigger web sites that are targeted, so if you're starting out small, maybe consider taking extra measures like the firewall and audits as you get more traffic and profit. (By Doug Norfolk)

SO CAN PEOPLE FEEL SAFE WHEN SHOPPING ON-LINE?

The answer to this is yes, if shoppers follow simple guidelines. If you are new to the Internet or a regular shopper online, the following guidelines should apply.

1. Make sure you know the exchange rate; if you are not sure of the current rates, find out before you buy an item.
2. Find out the cost of delivery before placing your order and how long the delivery will take. Most shopping sites use couriers to deliver the goods and when delivering overseas can become quite expensive.
3. If you are bidding on E-bay check out the buyers and sellers feedback. This should become standard before you ever place a bid.
4. Always read the FAQ section if you are new to the site.
5. If someone demands cash for a payment, 'say no'. Use your credit card to make your payment; this will protect you against fraud. Credit card companies refund accounts where fraudulent activity transpires.
6. Check the buyers contact page. Make sure their postal address is posted on it. If not, don't deal with them.
7. Don't be afraid to ask the seller lots of questions, genuine sellers should be very helpful, some online shopping sites have forms where you can see customer feed back.
8. Check, and read in full the terms and conditions, and the privacy policy of the site.
9. If you are unsure about a site, try doing a search with Google or any of the other search engines. You may find comments posted about the shopping site from other customers.
10. If you are still not sure after reading the above it may be time to go shopping elsewhere.

These simple guidelines should also apply when bidding online.

X. CONCLUSION

E-commerce is widely considered the buying and selling of products over the internet, but any transaction that is completed solely through electronic measures can be considered e-commerce. Day by day E-commerce and M-commerce playing very good role in online retail marketing and peoples using this technology day by day increasing all over the world.

E-commerce security is the protection of e-commerce assets from unauthorized access, use, alteration, or destruction. Dimensions of e-commerce security; Integrity: prevention against unauthorized data modification, No repudiation: prevention against any one party from reneging on an agreement after the fact. Authenticity: authentication of data source. Confidentiality: protection against unauthorized data

disclosure. Privacy: provision of data control and disclosure. Availability: prevention against data delays or removal.

Fraudsters are constantly looking to take advantage of online shoppers prone to making novice errors. Common mistakes that leave people vulnerable include shopping on websites that aren't secure, giving out too much personal information, and leaving computers open to viruses. In this paper we discussed E-commerce Security Issues, Security measures, Digital E-commerce cycle/Online Shopping, Security Threats and guidelines for safe and secure online shopping through shopping web sites.

XI. ACKNOWLEDGEMENT

I thank Dr. T. V. Suresh Kumar, Prof. and Head, Dept. of MCA, MSRIT, Bangalore-54. for his continuous support and encouragement for completing this research paper and also thanks to MSRIT management.

I thank Mr. S. Jagannatha , Associate Professor. Dept. of MCA, MSRIT, Bangalore-54. for his constant support and motivation.

XII. REFERENCES

[1] Mohanad Halaweh, Christine Fidler - " Security Perception in E-commerce: Conflict between Customer and Organizational Perspectives". Proceedings of the International Multiconference on Computer Science and Information Technology, pp. 443 – 449, ISBN 978-83-60810-14-9- 2008-IEEE

[2]Yuanqiao Wen, Chunhui Zhou "Research on E-Commerce Security Issues". 2008 International Seminar on Business and Information Management.

[3]Rui Wang, Shuo Chen "How to Shop for Free Online Security Analysis of Cashier-as-a-Service Based Web Stores". IEEE S&P'11 proceedings.

[4] V.SRIKANTH "ECOMMERCE ONLINE SECURITY AND TRUST MARKS". IJCET ISSN 0976 – 6375, Volume 3, Issue 2, July- September (2012),

[5] Shazia Yasin, Khalid Haseeb. "Cryptography Based E-Commerce Security: A Review". IJCSI-Vol. 9, Issue 2, No 1, March 2012

[6] Randy C. Marchany, Joseph G. Tront, "E-Commerce Security Issues"Proceedings of the 35th Hawaii International Conference on System Sciences - 2002

[7] Rashad Yazdanifard, Noor Al-Huda Edres "Security and Privacy Issues as a Potential Risk for Further Ecommerce Development"International Conference on Information Communication and Management - IPCSIT vol.16 (2011)

[8] Seyyed Mohammad Reza Farshchi "Study of Security Issues on Traditional and New Generation of E-commerce Model" International Conference on Software and Computer Applications-IPCSIT vol.9 (2011)

[9] RAJU BARSKAR, ANJANA JAYANT DEEN"The Algorithm Analysis of E-Commerce Security Issues for Online Payment Transaction System in Banking Technology"(IJCSIS)-Vol. 8, No. 1, April 2010

[10] Dr. Nada M. A. Al-Slamy, "E-Commerce security" IJCSNS - VOL.8 No.5, May 2008

[11] W. Jeberson, Prof. (Col.). Gurmit Singh. "Analysis of Security Measures Implemented on G2C Online Payment Systems in India" MIT International Journal of Computer Science & Information Technology Vol. 1 No. 1 Jan. 2011

[12] Abdulghader.A.Ahmed.Moftah. "CHALLENGES OF SECURITY, PROTECTION AND TRUST ON E-COMMERCE: A CASE OF ONLINE PURCHASING IN LIBYA". ISSN: 2278-1021-IJARCCE Vol. 1, Issue 3, May 2012.

[13] A SENGUPTA, C MAZUMDAR "e-Commerce security – A life cycle approach" Sadhana Vol. 30, Parts 2 & 3, April/June 2005

[14] Biswajit Tripathy, Jibitesh Mishra. "PROTECTIVE MEASURES IN E-COMMERCE TO DEAL WITH SECURITY THREATS ARISING OUT OF SOCIAL ISSUES – A FRAMEWORK" IAEME -ISSN 0976 – 6375(Online) Volume 4, Issue 1, January- February (2013),

[15] Pradnya B. Rane, Dr. B.B.Meshram. "Transaction Security for E-commerce Application" IJECSE -ISSN- 2277-1956. 2012

[16] Yang Jing "On-line Payment and Security of E-commerce". ISBN 978-952-5726-00-8 , 2009 International Symposium on Web Information Systems and Applications (WISA'09)

[17] Niranjanamurthy M, Kavyashree N, Mr S.Jagannath "M-COMMERCE: SECURITY CHALLENGES ISSUES AND RECOMMENDED SECURE PAYMENT METHOD" - IJMIE Volume 2, Issue 8 ISSN: 2249-0558 -2012

[18] Niranjanamurthy M, Kavyashree N, Mr S.Jagannath " E-COMMERCE AND M-COMMERCE: ISSUES AND RECOMMENDED SCREENING"- IJMT Volume 2, Issue 8 ISSN: 2249-1058 -2012

[19] Niranjanamurthy M, Kavyashree N, Mr S.Jagannath DR. Dharmendra Chahar. "Analysis of E-Commerce and M-Commerce: Advantages, Limitations and Security issues". IJARCCE-ISSN (Online) : 2278-1021. Vol. 2, Issue 6, June 2013