IJARCCE

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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 2, February 2016

Security Vulnerabilities and Solution for Electronic Commerce in Iraq

Huda Hamdan Ali[1], Hasan Abdulrazzaq Jawad[2]

Assistant Lecturer, Software Engineering Techniques, Imam Alkadhom University, Baghdad, Iraq[1, 2]

Abstract: Electronic commerce or e-commerce consists of the buying, selling, marketing, and servicing of products or services over computer networks. However, there are many risks and threats that happen in e-commerce. It is very important to improve the security on e- commerce business according to the high development and need on the internet business. Vulnerabilities in e–commerce in recently are also the main interesting for case study to explain how much e-commerce business security will be. This paper explain and discuss the e-commerce problems and suggestion for solution generally, taking e-commerce in Iraq as especial case, because the security for e-commerce is to make customers and business partners feel safe and comfortable when performing transactions. The basic principle is also important to make understanding about how security e-commerce. So e-commerce life cycle, security issues, e-commerce tool, threats and a set of suggestion for secure online shopping is discussed in this paper.

Keywords: e-commerce, security, vulnerabilities, e-business, protecting.

1. INTRODUCTION

Most of the problems facing online businesses are no different from those facing other organizations, and the network security risks are not much different from those facing traditional businesses. The real increased risks to an e-commerce have to do with ways in which traditional risk management mechanisms don’t scale properly from a world of local physical transactions to one of worldwide, dematerialized ones. Credit card transaction repudiation is the main example at present. There are also significant risks to rapidly growing companies that have hired a lot of new staff

There are many points of failure, or vulnerabilities, in an e-commerce environment. Even in a simplified e-commerce scenario – a single user contacts a single web site, and then gives his credit card and address information for shipping a purchase – many potential security vulnerabilities exist. Indeed, even in this simple scenario, there are a number of systems and networks involved. Each has security issues:

A user must use a web site and at some point identify, or authenticate, himself to the site. Typically, authentication begins on the user’s home computer and its browser. Unfortunately, security problems in home computers offer hackers other ways to steal e-commerce data and identification data from users. In the development of EC, security has always been the core and key issue that support its adoption[1]. Scholars believed that good security improves trust, and that the perceptions of good security and trust will ultimately increase the adoption and use of EC not just in the Arab countries but all over the world [2]. In fact, customers’ perceptions of the security and trust of e-payment systems, implemented by companies trading online, have become a major factor in the evolution of EC. It is clear, however, that the argument for the safety of consumer, and the end user has taken considerable reflections on the transaction importance [3]. Accordingly, an e-commerce merchant's first security priority should be to keep the web servers' archives of recent orders behind the firewall, not on the front-end web servers [4]. Furthermore, sensitive servers should be kept highly specialized, by turning off and removing all inessential services and applications (e.g., ftp, email). Other practical suggestions to secure web servers can be found in [5],A number of studies show that in a number of Arab countries; regarding EC, there is a slow acceptance of consumers` awareness of the benefits of using the Internet and see it as the spread of Western values and Western cultures [6]; [7]; [8].

Internet has caused several issues and problems in the Arab world and has been influencing as a major problem until the mid-1980s. Most consumers do not used to surf the Internet at home, but used to go to Internet cafes. Most users use Internet connections to make cheap long distance phone calls and chat.

We will discuss the implications of vulnerabilities below – users who may themselves release data or act in ways that place sites at jeopardy, the constant pressure of new technologies and the resulting constant threat of new vulnerabilities, as well as the requirements for critical organizational processes. However, before discussing potential requirements for e-commerce sites and their consumers, it is important to survey potential security technologies that don’t have the traditional internal controls in place.

2. DIGITAL E-COMMERCE CYCLE [9]

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

DOI 10.17148/IJARCCE.2016.5243

eBay, iTunes, Amazon, HMV, Mercantile, dell, Best Buy and much more.

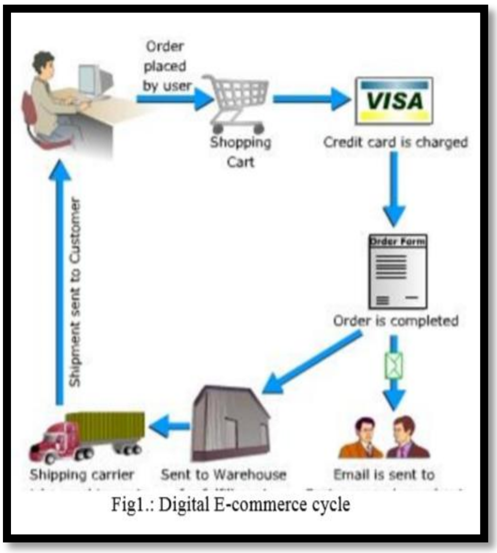

Fig1.: Digital E-commerce cycle

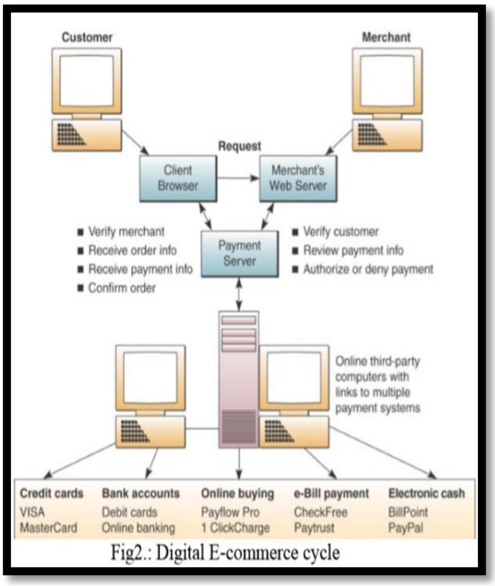

Fig2.: Digital E-commerce cycle

3. SECURITY ISSUES [10]

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 youare. 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 banking transactions.
- Auditing: Keeps a record of operations. Merchants use auditing to prove that you bought 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.

4. E-COMMERCE SECURITY TOOLS [11]

- ✓ 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.

5. SECURITY THREATS TO E-COMMERCE – REQUIREMENTS [12]

E-Commerce security requirements can be studied by examining the overall process, beginning with the consumer and ending with the commerce server. Considering each logical linking the “commerce chain”, the assets that must be protected to ensure secure e-commerce include client computers, the messages travelling on the communication channel, and the web and commerce servers – including any hardware attached to the servers. While telecommunications are certainly one of the major assets to be protected, the telecommunications links are not the only concern in computer and e-commerce security. For instance, if the telecommunications links were made secure but no security measures were implemented for either client computers or commerce and web-servers, then no communications security would exist at all.

5.1 Client threats

Until the introduction of executable web content, Web pages were mainly static. Coded in HTML, static pages could do little more than display content and provide links to related pages with additional information. However, the wide spread use of active content has changed this perception.

5.1a Active content: Active content refers to programs that are embedded transparently in web pages and that cause action to occur. Active content can display moving graphics, download and play audio, or implement web-based spreadsheet programs. Active content is use dine-commerce to place items one wishes to purchase into a shopping cart and to compute the total invoice amount, including sales tax, handling, and shipping costs. The best known active content forms are Java applets, ActiveX controls, JavaScript, and VBScript.

5.1b malicious codes: Computer viruses, worms and Trojan horses are examples of malicious code. ATrojan horse is a program which performs a useful function, but performs an unexpected action as well. Virus is a code segment which replicates by attaching copies to existing executables. A worm is a program which replicates itself and causes execution of the new copy. These can create havoc on the client side.

5.1c Server-side masquerading: Masquerading lures a victim into believing that the entity with which it is communicating is a different entity. For example, if a user tries to log into a computer across the internet but instead reaches another computer that claims to be the desired one, the user has been spoofed. This may be a passive attack (in which the user does not attempt to authenticate the recipient, but merely accesses it), but it is usually an active attack (in which the masquerader issues responses to mislead the user about its identity).

5.2 Communication channel threats

The internet serves as the electronic chain linking a consumer (client) to an e-commerce resource (commerce server). Messages on the internet travel a random path from a source node to a destination node. The message passes through a number of intermediate computers on the network before reaching the final destination. It is impossible to guarantee that every computer on the internet through which messages pass is safe, secure, and non-hostile.

5.2a Confidentiality threats: Confidentiality is the prevention of unauthorized information disclosure. Breaching confidentiality on the internet is not difficult. Suppose one logs onto a website – say www.anybiz.com – that contains a form with text boxes for name, address, and e-mail address.

5.2b Integrity threats: An integrity threat exists when an unauthorized party can alter a message stream of information. Unprotected banking transactions are subject to integrity violations.

5.2c Availability threats: The purpose of availability threats, also known as delay or denial threats, is to disrupt normal computer processing or to deny processing entirely. For example, if the processingspeed of asingle ATM machine transaction slows from one or two seconds to 30 seconds, users will abandon ATM machines entirely. Similarly, slowing any internet service will drive customers to competitors' web or commerce sites.

5.3 Server threats

The server is the third link in the client-internet-server trio embodying the e-commerce path between the user and a commerce server. Servers have vulnerabilities that can be exploited by anyone determined to cause destruction or to illegally acquire information.

5.3a Web-server threats: Web-server software is designed to deliver web pages by responding to HTTP requests. While web-server software is not inherently high-risk, it has been designed with web service and convenience as the main design goal. The more complex the software is, the higher the probability that it contains coding errors (bugs) and security holes – security weaknesses that provide openings through which evildoers can enter.

5.3b Commerce server threats: The commerce server, along with the web-server, responds to requests from web browsers through the HTTP protocol and CGI scripts. Several pieces of software comprise the commerce server software suite, including an FTP server, a mail server, a remote login server, and operating systems on host machines. Each of this software can have security holes and bugs.

5.3c Database threats: E-commerce systems store user data and retrieve product information from databases connected to the web-server. Besides product information, databases connected to the web contain valuable and private information that could irreparably dam- age a company if it were disclosed or altered. Some databases store username/password pairs in a non-secure way. If someone obtains user authentication information, then he or she can masquerade as a legitimate database user and reveal private and costly information.

5.3d Common gateway interface threats: A common gateway interface (CGI) implements the transfer of information from a web-server to another program, such as a database program. CGI and the programs to which they transfer data provide active content to web pages. Because CGIs are programs, they present a security threat if misused. Just like web-servers, CGI scripts can be set up to run with their privileges set to high – unconstrained. Defective or malicious CGIs with free access to system resources are capable of disabling the system, calling privileged (and dangerous) base system programs that delete files, or viewing confidential customer information, including usernames and passwords.

5.3e Password hacking: The simplest attack against a password-based system is to guess passwords. Guessing of passwords requires that access to the complement, the complementation functions, and the authentication functions be obtained. If none of these have changed by the time the password is guessed, then the attacker can use the password to access the system.

6. ADVANTAGES OF E-COMMERCE

The advantages of e-commerce for business entities can be summarized thus:

* E-commerce can increase sales and decrease costs.
*A firm can use e-commerce to reach narrow market segments that are widely scattered geographically.
*The internet and the web are particularly useful in creating virtual communities that become ideal target markets.
* A virtual community is a gathering of people who share a common interest, but, instead of this gathering occurring in the physical world; it takes place on the internet.
* Just as e-commerce increases sales opportunities for the seller, it increases purchasing opportunities for the buyer.
* Businesses can use e-commerce in their purchasing processes to identify new suppliers and business partners.
*Negotiating price and delivery terms is easier in e-commerce, because the web can provide competitive bid information very efficiently.
* E-Commerce increases the speed and accuracy with

DOI 10.17148/IJARCCE.2016.5243

which businesses can exchange information, which reduces costs on both sides of transactions.

* E-Commerce provides buyers with a wider range of choices than traditional commerce, because they can consider many different products and services from a wider variety of sellers.

* The benefits of e-commerce also extend to the general welfare of society.

* Electronic payments of tax refunds, public retirement, and welfare support cost less to issue and arrive securely and quickly when transmitted via the Internet.

*Furthermore, electronic payments can be easier to audit and monitor than payments made by check, which can help protect against fraud and theft losses.

*e-Commerce can make products and services available in remote areas. For example, distance education is making it possible for people to learn skills and earn degrees no matter where they live or what hours of the day they have available for study.

6.1 DISADVANTAGES OF E-COMMERCE

E-Commerce also has its disadvantages.

*It is difficult to conduct a few businesses electronically. For example, perishable foods and high-cost items such as jewelry or antiques may be impossible to adequately inspect from a remote location, regardless of the techneologies that are devised in the future.

* However, most of the disadvantages of e-commerce today are due to the newness and rapidly developing pace of the underlying technologies.

* Return on investment numbers is difficult to compute for investments in e-commerce, because the costs and benefits are hard to quantify.

*Costs, which are a function of technology, can change dramatically during even short-lived e-commerce implementation projects, because the underlying technologies change rapidly.

* In addition to technology issues, many businesses face cultural and legal impediments to e-commerce. Some consumers are still somewhat fearful of sending their credit card numbers over the Internet.

*The legal environment in which e-commerce is conducted is full of unclear and convicting glows. In many cases, government regulators have not kept up with technologies.

* As more businesses and individuals find the benefits of e-commerce compelling, many of these technology- and culture-related disadvantages will disappear. *Another importanttissues security.

*Transactions between buyers and seller sine-commerce include 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.

* The interception of transactions, and in particular credit card details, during transmission over the Internet is often a major obstacle to public confidence in e-commerce.

7. SUGGESTION FOR SECURE ONLINE SHOPPING

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

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 service or an order line. Call the phone number and ask questions to determine if the business is legitimate.

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.

4. Be Aware of Cookies and Behavioral 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.

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, seehttp://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.

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.

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

DOI 10.17148/IJARCCE.2016.5243

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 birthdates, 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 apotentially 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, 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.

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 thecompany'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 onthe 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 afterpurchasing on the Internet.Look for purchases you did not make. If you find some, immediately contact the credit card company and file a

DOI 10.17148/IJARCCE.2016.5243

dispute claim. 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.html.)

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. 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. 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 dynamicpricingsome 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.

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.

22. Additional Resources

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)

8. CONCLUSION

E-commerce in Iraq became more significant for the last five year, so the users faced big challenges and problems when they began dealing with e-commerce .especially with security threats and its solutions.

DOI 10.17148/IJARCCE.2016.5243

Most of the problems facing online businesses are no different from those facing other organizations, and the network security risks are not much different from those facing traditional businesses. The real increased risks to an e-business have to do with ways in which traditional risk management mechanisms don’t scale properly from a world of local physical transactions to one of worldwide, dematerialized ones. Credit card transaction repudiation is the main example at present. There are also significant risks to rapidly growing companies that have hired a lot of new staff but that don’t have the traditional internal controls in place.Many potential security vulnerabilities exist. And there are set of suggestion to avoid these vulnerabilities.

REFERENCES

[1] Zhang, Y. Deng, x. Wei, D. and Dengc, Y. (2012), “Assessment of E-Commerce security using AHP and evidential reasoning”, Experts Systems with Applications, Vol. 39. No. 3, pp. 3611 – 3623.

[2] Kima, Ch. Taoa, W. Shin, N. and Kima, S. (2010), “ An empirical study of customers’ perceptions of security and trust in e-payment system”, Electronic commerce Research and Applications, Vol. 9 No. 1. pp. 84-95

[3] Gray, V. (2001), “Barriers to Internet penetration in the Arab World” Arab Region Internet and Telecom Summit, Muscat, Oman, pp. 55-63.

[4] Warkentin, M., & Vaughn, R. (2006). Enterprise information systems assurance and system security: managerial and technical issues. Hershey: Idea Group Pub, pp. 45-59.

[5] Turban, E., Lee, J., King, D. and Viehland, D. (2006). E-commerce: A Managerial Perspective. Prentice Hall.

[6] Aladwani, A., (2003). “Key Internet characteristics and E-commerce issues in Arab countries.” Information Technology and People, Vol. 16, 1: 9-20.

[7] AlGhamdi, R & Drew, S (2011), 'Seven Key Drivers to Online Retailing in KSA', in P Kommers& P Isaías (eds), Proceedings of the IADIS International Conference on e-Society, Avila, Spain, pp. 237-44.

[8] Al-Mohamed, K,(2011), Information about e-mail for research use, E-mail communication edn, Riyadh.

[9] A Sengupta, C Mazumdar , M S Barik,(2006)," e-Commerce security – A life cycle approach", Sadhana, India, Vol. 30, Parts 2 & 3, pp. 119–140.

[10] Randy, Joseph,(2002),"E-Commerice Security Issues", Hawaii International Conference on System Sciences ,IEEE, vol 35,-7695 1435.

[11] Niranjanamurthy M, Dharmendra Chahar ,(2013)," The study of E-Commerce Security Issues and Solutions", International Journal of Advanced Research in Computer and Communication Engineering, India, Vol. 2, pp.2885-2895.

[12] Niranjana murthy M, Kavyashree N, Mr S. Jagannath, (2012)"Commerce: Security Challenges Issues and Recommended Secure Payment Method" - IJMIE Volume 2, Issue 8 ISSN: 2249-0558.

DOI 10.17148/IJARCCE.2016.5243