INTERNATIONAL JOURNAL OF RESEARCH IN COMMERCE, IT & MANAGEMENT

IJRCM

A Monthly Double-Blind Peer Reviewed (Refereed/Juried) Open Access International e-Journal - Included in the International Serial Directories

Indexed & Listed at:

Ulrich's Periodicals Directory ©, ProQuest, U.S.A., EBSCO Publishing, U.S.A., Cabell's Directories of Publishing Opportunities, U.S.A.,

Open J-Gage, India [link of the same is duly available at Inflibnet of University Grants Commission (U.G.C.)],

Index Copernicus Publishers Panel, Poland with IC Value of 5.09 & number of libraries all around the world.

Circulated all over the world & Google has verified that scholars of more than 3770 Cities in 175 countries/territories are visiting our journal on regular basis.

Ground Floor, Building No. 1041-C-1, Devi Bhawan Bazar, JAGADHRI – 135 003, Yamunanagar, Haryana, INDIA

http://ijrcm.org.in/

CONTENTS

CALL FOR MANUSCRIPTS

We invite unpublished novel, original, empirical and high quality research work pertaining to recent developments & practices in the areas of Computer Science & Applications; Commerce; Business; Finance; Marketing; Human Resource Management; General Management; Banking; Economics; Tourism Administration & Management; Education; Law; Library & Information Science; Defence & Strategic Studies; Electronic Science; Corporate Governance; Industrial Relations; and emerging paradigms in allied subjects like Accounting; Accounting Information Systems; Accounting Theory & Practice; Auditing; Behavioral Accounting; Behavioral Economics; Corporate Finance; Cost Accounting; Econometrics; Economic Development; Economic History; Financial Institutions & Markets; Financial Services; Fiscal Policy; Government & Non Profit Accounting; Industrial Organization; International Economics & Trade; International Finance; Macro Economics; Micro Economics; Rural Economics; Co-operation; Demography: Development Planning; Development Studies; Applied Economics; Development Economics; Business Economics; Monetary Policy; Public Policy Economics; Real Estate; Regional Economics; Political Science; Continuing Education; Labour Welfare; Philosophy; Psychology; Sociology; Tax Accounting; Advertising & Promotion Management; Management Information Systems (MIS); Business Law; Public Responsibility & Ethics; Communication; Direct Marketing; E-Commerce; Global Business; Health Care Administration; Labour Relations & Human Resource Management; Marketing Research; Marketing Theory & Applications; Non-Profit Organizations; Office Administration/Management; Operations Research/Statistics; Organizational Behavior & Theory; Organizational Development; Production/Operations; International Relations; Human Rights & Duties; Public Administration; Population Studies; Purchasing/Materials Management; Retailing; Sales/Selling; Services; Small Business Entrepreneurship; Strategic Management Policy; Technology/Innovation; Tourism & Hospitality; Transportation Distribution; Algorithms; Artificial Intelligence; Compilers & Translation; Computer Aided Design (CAD); Computer Aided Manufacturing; Computer Graphics; Computer Organization & Architecture; Database Structures & Systems; Discrete Structures; Internet; Management Information Systems; Modeling & Simulation; Neural Systems/Neural Networks; Numerical Analysis/Scientific Computing; Object Oriented Programming; Operating Systems; Programming Languages; Robotics; Symbolic & Formal Logic; Web Design and emerging paradigms in allied subjects.

Anybody can submit the **soft copy** of unpublished novel; original; empirical and high quality **research work/manuscript** ***anytime*** in ***M.S. Word format*** after preparing the same as per our **GUIDELINES FOR SUBMISSION**; at our email address i.e. infoijrcm@gmail.com or online by clicking the link **online submission** as given on our website (***FOR ONLINE SUBMISSION, CLICK HERE***).

GUIDELINES FOR SUBMISSION OF MANUSCRIPT

1. **COVERING LETTER FOR SUBMISSION:**

DATED: _____

THE EDITOR
IJRCM

Subject: **SUBMISSION OF MANUSCRIPT IN THE AREA OF.**

(e.g. Finance/Marketing/HRM/General Management/Economics/Psychology/Law/Computer/IT/Engineering/Mathematics/other, please specify)

DEAR SIR/MADAM

Please find my submission of manuscript entitled '_____' for possible publication in your journals.

I hereby affirm that the contents of this manuscript are original. Furthermore, it has neither been published elsewhere in any language fully or partly, nor is it under review for publication elsewhere.

I affirm that all the author (s) have seen and agreed to the submitted version of the manuscript and their inclusion of name (s) as co-author (s).

Also, if my/our manuscript is accepted, I/We agree to comply with the formalities as given on the website of the journal & you are free to publish our contribution in any of your journals.

NAME OF CORRESPONDING AUTHOR:
Designation:
Affiliation with full address, contact numbers & Pin Code:
Residential address with Pin Code:
Mobile Number (s):
Landline Number (s):
E-mail Address:
Alternate E-mail Address:

NOTES:

a) The whole manuscript is required to be in ***ONE MS WORD FILE*** only (pdf. version is liable to be rejected without any consideration), which will start from the covering letter, inside the manuscript.
b) The sender is required to mentionthe following in the **SUBJECT COLUMN** of the mail:
New Manuscript for Review in the area of (Finance/Marketing/HRM/General Management/Economics/Psychology/Law/Computer/IT/ Engineering/Mathematics/other, please specify)
c) There is no need to give any text in the body of mail, except the cases where the author wishes to give any specific message w.r.t. to the manuscript.
d) The total size of the file containing the manuscript is required to be below **500 KB**.
e) Abstract alone will not be considered for review, and the author is required to submit the complete manuscript in the first instance.
f) The journal gives acknowledgement w.r.t. the receipt of every email and in case of non-receipt of acknowledgment from the journal, w.r.t. the submission of manuscript, within two days of submission, the corresponding author is required to demand for the same by sending separate mail to the journal.

2. **MANUSCRIPT TITLE:** The title of the paper should be in a 12 point Calibri Font. It should be bold typed, centered and fully capitalised.

3. **AUTHOR NAME (S) & AFFILIATIONS:** The author (s) **full name**, **designation**, **affiliation** (s), **address**, **mobile/landline numbers**, and **email/alternate email address** should be in italic & 11-point Calibri Font. It must be centered underneath the title.

4. **ABSTRACT:** Abstract should be in fully italicized text, not exceeding 250 words. The abstract must be informative and explain the background, aims, methods, results & conclusion in a single para. Abbreviations must be mentioned in full.

5. **KEYWORDS:** Abstract must be followed by a list of keywords, subject to the maximum of five. These should be arranged in alphabetic order separated by commas and full stops at the end.

6. **MANUSCRIPT:** Manuscript must be in ***BRITISH ENGLISH*** prepared on a standard A4 size ***PORTRAIT SETTING PAPER***. It must be prepared on a single space and single column with 1" margin set for top, bottom, left and right. It should be typed in 8 point Calibri Font with page numbers at the bottom and centre of every page. It should be free from grammatical, spelling and punctuation errors and must be thoroughly edited.

7. **HEADINGS:** All the headings should be in a 10 point Calibri Font. These must be bold-faced, aligned left and fully capitalised. Leave a blank line before each heading.

8. **SUB-HEADINGS:** All the sub-headings should be in a 8 point Calibri Font. These must be bold-faced, aligned left and fully capitalised.

9. **MAIN TEXT:** The main text should follow the following sequence:

INTRODUCTION

REVIEW OF LITERATURE

NEED/IMPORTANCE OF THE STUDY

STATEMENT OF THE PROBLEM

OBJECTIVES

HYPOTHESES

RESEARCH METHODOLOGY

RESULTS & DISCUSSION

FINDINGS

RECOMMENDATIONS/SUGGESTIONS

CONCLUSIONS

SCOPE FOR FURTHER RESEARCH

ACKNOWLEDGMENTS

REFERENCES

APPENDIX/ANNEXURE

It should be in a 8 point Calibri Font, single spaced and justified. The manuscript should preferably not exceed ***5000 WORDS***.

10. **FIGURES &TABLES:** These should be simple, crystal clear, centered, separately numbered & self explained, and **titles must be above the table/figure**. **Sources of data should be mentioned below the table/figure**. It should be ensured that the tables/figures are referred to from the main text.

11. **EQUATIONS:**These should be consecutively numbered in parentheses, horizontally centered with equation number placed at the right.

12. **REFERENCES:** The list of all references should be alphabetically arranged. The author (s) should mention only the actually utilised references in the preparation of manuscript and they are supposed to follow **Harvard Style of Referencing**. The author (s) are supposed to follow the references as per the following:

- All works cited in the text (including sources for tables and figures) should be listed alphabetically.
- Use (**ed.**) for one editor, and (**ed.s)** for multiple editors.
- When listing two or more works by one author, use --- (20xx), such as after Kohl (1997), use --- (2001), etc, in chronologically ascending order.
- Indicate (opening and closing) page numbers for articles in journals and for chapters in books.
- The title of books and journals should be in italics. Double quotation marks are used for titles of journal articles, book chapters, dissertations, reports, working papers, unpublished material, etc.
- For titles in a language other than English, provide an English translation in parentheses.
- The location of endnotes within the text should be indicated by superscript numbers.

PLEASE USE THE FOLLOWING FOR STYLE AND PUNCTUATION IN REFERENCES:

BOOKS

- Bowersox, Donald J., Closs, David J., (1996), "Logistical Management." Tata McGraw, Hill, New Delhi.
- Hunker, H.L. and A.J. Wright (1963), "Factors of Industrial Location in Ohio" Ohio State University, Nigeria.

CONTRIBUTIONS TO BOOKS

- Sharma T., Kwatra, G. (2008) Effectiveness of Social Advertising: A Study of Selected Campaigns, Corporate Social Responsibility, Edited by David Crowther & Nicholas Capaldi, Ashgate Research Companion to Corporate Social Responsibility, Chapter 15, pp 287-303.

JOURNAL AND OTHER ARTICLES

- Schemenner, R.W., Huber, J.C. and Cook, R.L. (1987), "Geographic Differences and the Location of New Manufacturing Facilities," Journal of Urban Economics, Vol. 21, No. 1, pp. 83-104.

CONFERENCE PAPERS

- Garg, Sambhav (2011): "Business Ethics" Paper presented at the Annual International Conference for the All India Management Association, New Delhi, India, 19–22 June.

UNPUBLISHED DISSERTATIONS AND THESES

- Kumar S. (2011): "Customer Value: A Comparative Study of Rural and Urban Customers," Thesis, Kurukshetra University, Kurukshetra.

ONLINE RESOURCES

- Always indicate the date that the source was accessed, as online resources are frequently updated or removed.

WEBSITES

- Garg, Bhavet (2011): Towards a New Natural Gas Policy, Political Weekly, Viewed on January 01, 2012 http://epw.in/user/viewabstract.jsp

SECURITY ISSUES IN e-COMMERCE

DR. SARITA MUNDRA
ASST. PROFESSOR
SHRI CLOTH MARKET GIRLS COMMERCE COLLEGE
INDORE

DR. SADHANA ZANZARI
ASST. PROFESSOR
SHRI CLOTH MARKET GIRLS COMMERCE COLLEGE
INDORE

ER. SURABHI MUNDRA
ALUMNI
SHRI G. S. INSTITUTE OF TECHNOLOGY AND SCIENCE
INDORE

ABSTRACT

E-commerce security is the protection of e-commerce assets from unauthorized access, use, alteration, or destruction. It is a part of the information security framework and is specifically applied to the components that affect e-commerce. Dimensions of e-commerce security are integrity, non-repudiation, authenticity, confidentiality, privacy, availability. Today's consumer is confronted by a maze of different online commerce opportunities, choices, and decisions, none of which were available or even fathomable 20 years ago. E-commerce is gaining momentum and acceptance; previously risky online activities such as banking are now considered safe and reliable, yet popular methods used to access sensitive information online present serious security risks.[6] Most consumers accept terms and conditions too easily and without a second thought, compromising online anonymity and privacy. E-commerce isn't just increasing, it's evolving. The exponential rate of e-commerce growth has far surpassed mainstream security measures set in place to properly regulate online commerce and prevent consumer identity fraud. Every time a new e-commerce innovation is released, a new security risk is posed for consumers. To ensure the security, privacy and effectiveness of e-commerce, on one hand businesses should authenticate business transactions, control access to resources such as web pages for registered or selected users, encrypt communications and implement security technologies, while on other hand consumers need to be cautious and attentive to minute details.[4]

KEYWORDS

e-commerce, information security.

1. INTRODUCTION TO e-COMMERCE

E-commerce (electronic commerce or ec) is the buying and selling of goods and services, or the transmitting of funds or data, over an electronic network, primarily the internet. These business transactions occur either business-to-business, business-to-consumer, consumer-to-consumer or consumer-to-business. The terms *e-commerce* and *e-business* are often used interchangeably. The term *e-tail* is also sometimes used in reference to transactional processes around online retail.[4]

E-commerce is conducted using a variety of applications, such as email, fax, online catalogs and shopping carts, electronic data interchange (edi), file transfer protocol, and web services. Most of this is business-to-business, with some companies attempting to use email and fax for unsolicited ads (usually viewed as spam) to consumers and other business prospects, as well as to send out e-newsletters to subscribers.

The benefits of e-commerce include its around-the-clock availability, the speed of access, a wider selection of goods and services, accessibility, and international reach. Its perceived downsides include sometimes-limited customer service, not being able to see or touch a product prior to purchase, and the necessitated wait time for product shipping.

2. PURPOSE OF STUDY

- Study the overview of e-commerce security
- Discuss the threats to e-commerce security
- Understand the tools for e-commerce security
- Understand the secure online shopping guidelines

3. e-COMMERCE SECURITY

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 domains of the information security framework. 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 e-commerce. The e-commerce industry is slowly addressing security issues on their internal networks. There are guidelines for securing systems and networks available for the e-commerce 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.[1]

Security is an essential part of any transaction that takes place over the internet. Customer will lose his/her faith in e-business if its security is compromised.[7]

Following are the essential requirements for safe e-payments/transactions:

Confidentiality: Information should not be accessible to unauthorized person. It should not be intercepted during transmission.

Integrity: Information should not be altered during its transmission over the network.

Authenticity: There should be a mechanism to authenticate user before giving him/her access to required information.

Non-repudiability: It is protection against denial of order or denial of payment. Once a sender sends a message, the sender should not able to deny sending the message. Similarly the recipient of message should not be able to deny receipt.

Encryption: Information should be encrypted and decrypted only by authorized user.

4. e-COMMERCE SECURITY THREATS

The direct threats to e-commerce servers can be classified as malicious code threats and transmission threats. [3]Malicious or rogue programming code is introduced into the server in order to gain access to the system resources. Very often, the intent of malicious code attacks is to cause large scale damage to the e-commerce server. With transmission threats, the threats and risks can be classified as either as active or passive. With passive threats, the main goal is to listen (or eavesdrop) to transmissions to the server. With active threats, the intent is to alter the flow of data transmission or to create a rogue transmission aimed directly at the e-commerce server.

MALICIOUS CODE ATTACKS

Viruses and worms: A virus attaches itself to executable code and is executed when the software program begins to run or an infected file is opened. However, a worm does not need a host to replicate. Rather, the worm replicates itself through the internet, and can literally infect millions of computers on a global basis in just a matter of hours. Worms by themselves do not cause damage to a system like a virus does. However, worms can shut down parts of the internet or e-commerce servers, because they can use up valuable resources of the internet, as well as the memory and processing power of servers and other computers.

Trojan horses: A Trojan horse is a piece of programming code that is layered behind another program, and can perform covert, malicious functions. For example, your e-commerce server can display a "cool-looking" screen saver, but behind that could be a piece of hidden code, causing damage to your system. One way to get a Trojan horse attack is by downloading software from the internet. Make sure that whatever software is downloaded comes from an authentic and verified source, and that all defense mechanisms are activated on your server.

Logic bombs: A logic bomb is a version of a Trojan horse, however, it is event or time specific. For example, a logic bomb will release malicious or rogue code in an e-commerce server after some specific time has elapsed or a particular event in application or processing has occurred.

TRANSMISSION THREATS

Denial of service attacks: With a denial of service attack, the main intention is to deny your customers the services provided on your e-commerce server. This happens when a massive amount of invalid data is sent to the server. Because the server can handle and process so much information at any given time, it is unable to keep with the information and data overflow. As a result, the server becomes "confused", and subsequently shuts down.

Ping of death: With a ping of death attack, a massive data packet is sent to the server. As a result, the memory buffers of the e-commerce server are totally overloaded, thus causing it to crash.

SYN flooding: A SYN flood is a form of denial-of-service attack in which an attacker sends a succession of SYN requests to a target's system in an attempt to consume enough server resources to make the system unresponsive to legitimate traffic

Ip spoofing: The intent here is to change the source address of a data packet to give it the appearance that it originated from another computer. With ip spoofing, it is difficult to identify the real attacker, since all e-commerce server logs will show connections from a legitimate source.

5. e-COMMERCE SECURITY TOOLS

Firewalls: (for software and hardware): A firewall is a system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized internet users from accessing private networks connected to the internet, especially intranets. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

Public key infrastructure: A pki (public key infrastructure) enables users of a basically unsecure public network such as the internet to securely and privately exchange data and money through the use of a public and a private cryptographic key pair that is obtained and shared through a trusted authority.

Encryption software: Encryption software is software whose main task is encryption and decryption of data, usually in the form of files on (or sectors of) hard drives and removable media, email messages, or in the form of packets sent over computer networks. It is a very effective and practical way to safeguard the data being transmitted over the network. Sender of the information encrypts the data using a secret code and specified receiver only can decrypt the data using the same or different secret code.

Digital signature: Digital signature ensures the authenticity of the information. A digital signature is a e-signature authentic authenticated through encryption and password.

Security certificates: Security certificate is unique digital id used to verify identity of an individual website or user.

6. GUIDELINES TO SHOP ONLINE SAFELY

SHOP AT SECURE WEB SITES

A secure web site uses encryption and authentication standards to protect the confidentiality of information sent during web transactions. A secure web page can be identified using following guidelines:

1. The url of a secure webpage begins with the letters https
2. Ensure that the address bar has some element of green in it. Different browsers use different elements. Microsoft's internet explorer - background is shaded green. Apple's safari and google's chrome - https is shaded green
3. Look for a closed padlock. If that lock is open, you should assume it is not a secure site. Most web browsers display the 'lock' icon somewhere in the window of the browser. Microsoft's internet explorer displays a lock in the lower-right of the browser window. Mozilla's firefox displays the lock icon in the lower-left corner of the window. The lock is not just a picture. You can click or double click on it to see details of the site's security. This is important because some fraudulent sites are built with a bar at the bottom of the page to imitate the lock icon of your browser.

INVESTIGATE ABOUT THE WEB SITE BEFORE YOU ORDER

Avoid doing business with unknown *web sites*. If you are going to deal with a web site for the first time, do your homework before buying their products. Start business with an unknown website by ordering something inexpensive. This will help you judge the authenticity of the web site.

Reliable *web sites* should advertise their physical business address and contact number, either customer service or an order line. Call the phone number and ask questions to determine if the business is legitimate.

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.[8] Reputable companies will be open about how they collect data from you and what they do with it. Many now also belong to web-seal approval or trust mark programs that set out guidelines on the treatment of your information.

USE SAFE PAYMENT OPTIONS

Credit cards are generally the safest option because they allow buyers to seek a credit from the issuer if the product isn't delivered or isn't what was ordered. [9]Also, unlike debit cards, credit cards may have a limit on the monetary amount you will be responsible for paying if your information is stolen and used by someone else. Never send cash through the mail or use a money-wiring service because you'll have no recourse if something goes wrong. Don't forget to review return policies. You want a no-hassle ability to return items.

USE VIRTUAL CREDIT CARDS AS NEEDED

Virtual credit cards are temporary payment cards, and come in the form of a physical plastic card, or as a generated credit card number, and they're separate from your bank information.[10] This type of disposable credit card payment method contains a pre-set spending amount, has a shorter-than-usual expiration date, and is equivalent to a regular credit card for most payments purposes. Virtual credit card payments are usually charged to your credit or debit card, rather than directly to your bank account, essentially offering an additional layer of protection. When you pay with a virtual credit card, your banking information remains separate from your individual purchase, thus ensuring if the card number is stolen, hackers cannot access your accounts or re-use the card fraudulently.

DISCLOSE ONLY THE BARE FACTS WHEN YOU ORDER

When making a purchase online, 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. Be alert to the kinds of information being collected to complete the transaction. Make sure you think it is necessary for the vendor to request that information. Remember, you only need to fill out required fields on a vendors checkout form. Before providing personal or financial information, make sure you understand how your information will be stored and used. The information you provide 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 (*).

KEEP YOUR PASSWORD PRIVATE

You will usually be asked for a password before you make an online payment. This is to help keep your personal details private.[11] Make sure you use a strong password - one that is a combination of letters (upper and lower case), numbers and symbols. 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.

DON'T FALL FOR "PHISHING" MESSAGES

Phishing is the process whereby someone attempts to obtain your confidential information, such as your passwords, your credit card number, your bank account details or other information protected by the data protection act. [12]A phishing attack can be in the form of an official looking email or instant message, maybe directing you to an official looking website, or it could be an official sounding phone call.

Recognizing a phishing attack

There are number of clues that may indicate an email or website is not genuine such as:

1. Suspicious email links. Try hovering your mouse over a link without clicking on it. If the address that pops up does not match the link address as it is written in the email, it's a clear indication of a phishing email.
2. A link to a genuine website which takes you somewhere else
3. Spelling or grammatical mistakes, inappropriate use of capitals or exclamation marks, formatting errors
4. A generic email greeting
5. Claims that you need to act immediately to prevent something bad from happening (for example, your account will be deleted or your email will be lost)
6. Requests for personal information, such as your password or bank account number

However, you should always be wary as some phishing attacks may be sophisticated and difficult to spot. You should refuse to disclose confidential information until you have checked to your own satisfaction that the request is justified and legitimate and has been made by a genuine person or organization.

There are various phishing filters, like smartscreen filter in internet explorer, which will help protect you from phishing sites by warning you when it detects a distrustful website.

ALWAYS PRINT OR SAVE COPIES OF YOUR ORDERS

Print and save records of your online transactions, including the product description, price, online receipt, terms of the sale, and copies of any email exchange with the seller.[9] If you cannot print one off, take a screenshot as a form of proof of purchase. 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. Read your credit card statements as soon as you get them to make sure there aren't any unauthorized charges. If there is a discrepancy, call your bank and report it immediately

TURN YOUR COMPUTER OFF WHEN YOU'RE FINISHED SHOPPING

Many people leave their computers running and connected to the internet all day and night. This gives scammers 24/7 access to your computer to install malware and commit cyber crimes. To be safe, turn off your computer when it's not in use.

FIND OUT ABOUT BILLING, GUARANTEES, CANCELLATION POLICIES, SHIPPING AND DELIVERY CHARGES BEFORE YOU BUY

You can look for following information: [13]

1. Packaging costs, delivery costs etc
2. Whether you will be billed before or after delivery of the products
3. Whether you can track the item from the moment of purchase to arrival at your door - this will help alert you of any hiccups in the delivery
4. Whether the product comes with a guarantee or warranty for defects etc.
5. How you can return the product if it doesn't work or meet your expectations - look for information on the site about cancellations, returns and refunds. Print off a copy for future reference
6. Who will bear the cost of returning the item (postage, fees etc.)

KNOW HOW ONLINE AUCTIONS OPERATE

Online auctions connect buyers and sellers, allowing them to communicate in a bidding process over items for sale.[13] For the most part, online auction sites are a safe way to exchange goods. But it makes sense to be cautious and aware.

Online auctions can be a lot of fun and can also help you find good deals. They also attract scammers. Scammers will often try to get you to deal outside of online auction sites. They may claim the winner of an auction that you were bidding on has pulled out and offer the item to you. Once you have paid, you will never hear from them again and the auction site will not be able to help you. Following are the guidelines for participating safely in online auctions:

1. Always conduct transactions within the auction website and avoid private contact with buyers or sellers-scammers will often use this ploy to 'offer a better deal'.
2. Keep printed and/or electronic records of all bids, item descriptions, emails to and from the seller, and transaction records or receipts.
3. If the website uses a feedback rating system, check all comments left by previous buyers and sellers.
4. Use a secure payment method.
5. Avoid money transfers and direct debit, because they can be open to abuse.
6. Consider using the insurance offered by the auction facility.
7. Check the information on auction websites to help potential buyers and sellers.
8. Take the time to read the information about ways to reduce the risk on the auction site and the terms and conditions of contracts entered into by bidders and sellers.
9. 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.

BE AWARE OF DYNAMIC PRICING

Dynamic pricing is a blanket term for any shopping experience where the price of an item fluctuates frequently based on complicated algorithms.[14] Some online retailers use dynamic pricing to engage in price discrimination by charging different prices to different consumers for identical goods or services. 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.

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 they visit the issuer's site.

Shared wi-fi = unsecure wi-fi

As a rule of thumb, assume all shared wi-fi networks are unsafe for your sensitive data. Everything from an online bank statement to a gmail account can be compromised when surfing the web on a shared wi-fi network. It's nearly impossible to accurately gauge how secure a wi-fi network is, and thus it's best to err on the side of caution. [15]

PROTECT YOUR ONLINE IDENTITY ON THE SOCIAL FRONT

Online purchasing is getting more and more social, with 50 per cent of web sales projected to occur via social media by 2015. [15]Each time you join a new site through the "login with facebook" option, you're extending your online identity further. In fact, an abundance of sites will first prompt you to become a member not by email, but by connecting a social media account. Is it a direct connection? Technically, no. Will it be used to shape your online identity? Absolutely. Your social media presence defines your digital footprint to the point where companies are looking to use your social media identity to combat online payment fraud and your social signals to tackle identity fraud in the near future.

Once you realize that the majority of your online activity is interconnected, you can better defend yourself from making thoughtless choices that may endanger your data. Just like you shouldn't post something you don't want your employer to see on facebook, you also shouldn't post anything you don't want a hacker to see, like a picture of your driver's license or passport, anything with a home address and any snapshots that include a visible credit card or credit card number.

7. CONCLUSION

Day by day e-commerce is playing a very vital role in online retail marketing and the number of people using this technology is increasing in leaps and bounds all over the world. However the exponential rate of e-commerce growth has lead to numerous security risks for consumers. In present scenario, consumer needs to be very cautious while making any kind of online transactions or even surfing the internet.

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 threats and guidelines for safe and secure online shopping through shopping web sites. A consumer can very well secure his online shopping to some extend by religiously following the guidelines mentioned in the research paper.

REFERENCES

1. Niranjanamurthy M 1, DR. Dharmendra Chahar - “The study of E-Commerce Security Issues and Solutions”, International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 7, July 2013
2. Raghav Gautam, “ Network Security Issues in e-Commerce”, Volume 4, Issue 3, March 014 ISSN: 2277 128X, International Journal of Advanced Research in Computer Science and Software Engineering
3. Threats to E-Commerce Servers-Part I http://www.technologyexecutivesclub.com/Articles/security/artThreatstoEcommerceServers.php
4. e-commerce (electronic commerce or EC) http://searchcio.techtarget.com/definition/e-commerce
5. Online Shopping Tips: E-Commerce and You https://www.privacyrights.org/online-shopping-tips-e-commerce-and-you
6. 5 E-Commerce Security Tips http://www.pcmag.com/article2/0,2817,2421846,00.asp
7. E-Commerce Security Systems http://www.tutorialspoint.com/e_commerce/e_commerce_security.htm
8. How to shop online without a credit card http://shoppingonline-tips.blogspot.in/2014_07_01_archive.html
9. Online Shopping http://www.staysafeonline.org/stay-safe-online/protect-your-personal-information/online-shopping
10. E-commerce security tips: How to stay safe when shopping online http://www.itproportal.com/2013/07/18/e-commerce-security-tips-how-to-stay-safe-when-shopping-online/
11. How to shop safely and securely online http://www.bbc.co.uk/webwise/0/22728224
12. Beware of Phishing http://www2.le.ac.uk/offices/ias/topics/phishing
13. Fact Sheet 23: Online Shopping Tips: E-Commerce and You https://www.privacyrights.org/online-shopping-tips-e-commerce-and-you
14. Everything you need to know about dynamic pricing http://www.csmonitor.com
15. E-commerce security tips http://www.itproportal.com/2013/07/18/e-commerce-security-tips-how-to-stay-safe-when-shopping-online/

REQUEST FOR FEEDBACK

Dear Readers

At the very outset, International Journal of Research in Commerce, IT & Management (IJRCM) acknowledges & appreciates your efforts in showing interest in our present issue under your kind perusal.

I would like to request you tosupply your critical comments and suggestions about the material published in this issue as well as on the journal as a whole, on our E-mail**infoijrcm@gmail.com** for further improvements in the interest of research.

If youhave any queries please feel free to contact us on our E-mail infoijrcm@gmail.com.

I am sure that your feedback and deliberations would make future issues better – a result of our joint effort.

Looking forward an appropriate consideration.

With sincere regards

Thanking you profoundly

Academically yours

Sd/-
Co-ordinator

DISCLAIMER

The information and opinions presented in the Journal reflect the views of the authors and not of the Journal or its Editorial Board or the Publishers/Editors. Publication does not constitute endorsement by the journal. Neither the Journal nor its publishers/Editors/Editorial Board nor anyone else involved in creating, producing or delivering the journal or the materials contained therein, assumes any liability or responsibility for the accuracy, completeness, or usefulness of any information provided in the journal, nor shall they be liable for any direct, indirect, incidental, special, consequential or punitive damages arising out of the use of information/material contained in the journal. The journal, nor its publishers/Editors/ Editorial Board, nor any other party involved in the preparation of material contained in the journal represents or warrants that the information contained herein is in every respect accurate or complete, and they are not responsible for any errors or omissions or for the results obtained from the use of such material. Readers are encouraged to confirm the information contained herein with other sources. The responsibility of the contents and the opinions expressed in this journal is exclusively of the author (s) concerned.

ABOUT THE JOURNAL

In this age of Commerce, Economics, Computer, I.T. & Management and cut throat competition, a group of intellectuals felt the need to have some platform, where young and budding managers and academicians could express their views and discuss the problems among their peers. This journal was conceived with this noble intention in view. This journal has been introduced to give an opportunity for expressing refined and innovative ideas in this field. It is our humble endeavour to provide a springboard to the upcoming specialists and give a chance to know about the latest in the sphere of research and knowledge. We have taken a small step and we hope that with the active co-operation of like-minded scholars, we shall be able to serve the society with our humble efforts.

Our Other Journals