

INTERNATIONAL JOURNAL OF RESEARCH IN COMMERCE, IT & MANAGEMENT

I
J
R
C
M



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-Gate, India [link of the same is duly available at Inlibnet 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 3130 Cities in 166 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

Sr. No.	TITLE & NAME OF THE AUTHOR (S)	Page No.
1.	A STUDY OF IMPORTANCE OF ETIQUETTES FOR A PROFESSIONAL <i>DR. G. SUNITHA & A. K. NEERAJA RANI</i>	1
2.	COPYRIGHT PROTECTION FOR RGB WATERMARK IMAGE USING IN LSB <i>RAJNI VERMA & ARCHNA TIWARI</i>	4
3.	HOW LEADERSHIP AFFECTS ORGANIZATIONAL CHANGE PROCESS <i>RAJA MUHAMMAD YASIR & DR. HUMAYOUN NAEEM</i>	10
4.	FACTORS INFLUENCING CUSTOMERS' LOYALTY IN ONLINE SHOPPING <i>TUSHAR BHAVSAR & DR. RAJESH M. PATEL</i>	13
5.	A STUDY ON THE ROLE OF EMOTIONAL SATISFACTION IN RETAIL OUTLETS <i>T. KALAKUMARI & DR. M. SEKAR</i>	16
6.	STAFF ATTITUDES TO SHELVING AND SHELF READING IN PUBLIC LIBRARIES IN NIGERIA <i>JOHN MUYIWA ADENIYI CLN</i>	20
7.	A ROAD MAP TOWARDS SECURE CYBER WORLD <i>SANDEEP YADAV</i>	22
8.	FDI IN RETAIL: BOON OR BANE <i>ANNU AGGARWAL</i>	25
9.	WORKING CAPITAL MANAGEMENT AND ITS IMPACT ON PROFITABILITY: A CASE STUDY OF DR. REDDY'S LABORATORIES LTD. <i>NIRMAL CHAKRABORTY</i>	33
10.	QUALITATIVE ANALYSIS OF FDI IN INDIAN RETAIL INDUSTRY <i>PALLAVI MANIK & RENU SINGLA</i>	38
11.	e-COMMERCE IN PUBLIC SECTOR BANKS <i>IYER SEETHALAKSHMI BALAKRISHNAN</i>	42
12.	CREATING COMPETITIVE ADVANTAGE THROUGH SUPPLY CHAIN MANAGEMENT (ROLE OF INFORMATION & COMMUNICATION TECHNOLOGY IN SUPPLY CHAIN MANAGEMENT TO CREATE COMPETITIVE ADVANTAGE: A LITERATURE BASE STUDY) <i>SAIF MAQBOOL, MUHAMMAD RAFIQ, MUHAMMAD IMRAN, ABDUL QADEER & TAJAMMAL ABBAS</i>	47
13.	ADOPTION OF INFORMATION TECHNOLOGY AND BANKS PERFORMANCE: A SURVEY OF SELECTED BANKS IN NIGERIA <i>SAMSON YIMKA ALALADE, KEMI OMONIYI & BOLANLE O. AMUSA</i>	53
14.	A STUDY OF UNDERGRADUATE COLLEGE STUDENT'S STUDY HABITS IN RELATION TO THEIR ACADEMIC ACHIEVEMENT <i>ISHRAT NAAZ</i>	60
15.	PACKAGING DESIGN AS NEW INNOVATIVE PROMOTIONAL TOOL <i>SHRUTI CHAUDHARY</i>	65
	REQUEST FOR FEEDBACK & DISCLAIMER	69

CHIEF PATRON

PROF. K. K. AGGARWAL

Chairman, Malaviya National Institute of Technology, Jaipur
(An institute of National Importance & fully funded by Ministry of Human Resource Development, Government of India)
Chancellor, K. R. Mangalam University, Gurgaon
Chancellor, Lingaya's University, Faridabad
Founder Vice-Chancellor (1998-2008), Guru Gobind Singh Indraprastha University, Delhi
Ex. Pro Vice-Chancellor, Guru Jambheshwar University, Hisar

FOUNDER PATRON

LATE SH. RAM BHAJAN AGGARWAL

Former State Minister for Home & Tourism, Government of Haryana
Former Vice-President, Dadri Education Society, Charkhi Dadri
Former President, Chinar Syntex Ltd. (Textile Mills), Bhiwani

CO-ORDINATOR

AMITA

Faculty, Government M. S., Mohali

ADVISORS

DR. PRIYA RANJAN TRIVEDI

Chancellor, The Global Open University, Nagaland

PROF. M. S. SENAM RAJU

Director A. C. D., School of Management Studies, I.G.N.O.U., New Delhi

PROF. M. N. SHARMA

Chairman, M.B.A., Haryana College of Technology & Management, Kaithal

PROF. S. L. MAHANDRU

Principal (Retd.), Maharaja Agrasen College, Jagadhri

EDITOR

PROF. R. K. SHARMA

Professor, Bharti Vidyapeeth University Institute of Management & Research, New Delhi

CO-EDITOR

DR. BHAVET

Faculty, Shree Ram Institute of Business & Management, Urjani

EDITORIAL ADVISORY BOARD

DR. RAJESH MODI

Faculty, Yanbu Industrial College, Kingdom of Saudi Arabia

PROF. SANJIV MITTAL

University School of Management Studies, Guru Gobind Singh I. P. University, Delhi

PROF. ANIL K. SAINI

Chairperson (CRC), Guru Gobind Singh I. P. University, Delhi

DR. SAMBHAVNA

Faculty, I.I.T.M., Delhi

DR. MOHENDER KUMAR GUPTA

Associate Professor, P. J. L. N. Government College, Faridabad

DR. SHIVAKUMAR DEENE

Asst. Professor, Dept. of Commerce, School of Business Studies, Central University of Karnataka, Gulbarga

ASSOCIATE EDITORS

PROF. NAWAB ALI KHAN

Department of Commerce, Aligarh Muslim University, Aligarh, U.P.

PROF. ABHAY BANSAL

Head, Department of Information Technology, Amity School of Engineering & Technology, Amity University, Noida

PROF. A. SURYANARAYANA

Department of Business Management, Osmania University, Hyderabad

DR. SAMBHAV GARG

Faculty, Shree Ram Institute of Business & Management, Urjani

PROF. V. SELVAM

SSL, VIT University, Vellore

DR. PARDEEP AHLAWAT

Associate Professor, Institute of Management Studies & Research, Maharshi Dayanand University, Rohtak

DR. S. TABASSUM SULTANA

Associate Professor, Department of Business Management, Matrusri Institute of P.G. Studies, Hyderabad

SURJEET SINGH

Asst. Professor, Department of Computer Science, G. M. N. (P.G.) College, Ambala Cantt.

TECHNICAL ADVISOR

AMITA

Faculty, Government M. S., Mohali

FINANCIAL ADVISORS

DICKIN GOYAL

Advocate & Tax Adviser, Panchkula

NEENA

Investment Consultant, Chambaghat, Solan, Himachal Pradesh

LEGAL ADVISORS

JITENDER S. CHAHAL

Advocate, Punjab & Haryana High Court, Chandigarh U.T.

CHANDER BHUSHAN SHARMA

Advocate & Consultant, District Courts, Yamunanagar at Jagadhri

SUPERINTENDENT

SURENDER KUMAR POONIA

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 mention the 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>

e-COMMERCE IN PUBLIC SECTOR BANKS**IYER SEETHALAKSHMI BALAKRISHNAN****ASST. PROFESSOR****VPM'S K.G. JOSHI COLLEGE OF ARTS & N.G. BEDEKAR COLLEGE OF COMMERCE****CHENDANI****ABSTRACT**

Today it can be observed that the financial liberalization and technology revolution have allowed the developments of new and more efficient delivery and processing channels as well as more innovative products and services in banking industry. Banking institutions are facing competition not only from each other but also from non-bank financial intermediaries as well as from alternative sources of financing. As financial institutions increasingly offer online banking services to their customers, they must face issues of consumer confidence in the Internet. Consumers are concerned about identity theft and wonder if the Internet is safe for online banking. Therefore, building the best controls to prevent fraud and protect customers is of critical importance. This paper investigates the extent of safety measures followed by customers while e-banking, analyses the awareness of the customers regarding the various online banking scams and suggests safety measures to be followed while e-banking. Primary data was collected from 50 respondents through a structured questionnaire. Secondary data was used to know about the various electronic e-banking products and services and various online scams. It is anticipated that the findings would be useful to the banking sector to frame proper policies in the area of e-banking.

KEYWORDS

E-banking, online scams, safety measures.

INTRODUCTION

Indian banking is the lifeline of the nation and its people. Banking has helped in developing the vital sectors of the economy and usher in a new dawn of progress on the Indian horizon. The sector has translated the hopes and aspirations of millions of people into reality. But to do so it has to control miles and miles of difficult terrain, suffer the indignities of foreign rule and the pangs of partition. Today, Indian banks can confidently compete with modern banks of the world. As the banking institutions expand and become increasingly complex under the impact of deregulation, innovation and technological up gradation, it is crucial to maintain balance between efficiency and stability. During the last 30 years since nationalization tremendous changes have taken in the financial markets as well as in the banking industry due to financial sector reforms. The banks have shed their traditional functions and have been innovating, improving and coming out with new types of services to cater to the emerging needs of their customers. Banks have been given greater freedom to frame their own policies. Rapid advancement of technology has contributed to significant reduction in transaction costs, facilitated greater diversification of portfolio and improvements in credit delivery of banks. During the past one decade, one of the sectors which underwent visible sea-change through innovative strategies is undoubtedly the banking sector. The sector has been growing at a fast pace in India and is challenged with several aspects like new regulations from time to time, changing customer needs and perceptions, changing technology and changing operations. Technology has been playing a crucial role in the tremendous improvement of banking services and operations. Banks appear to be on the path of achieving sustainability and a long term survival because of innovation. Technological changes relating to telecommunications and data processing have spurred financial innovations that have altered bank products and services and production processes.

STATEMENT OF THE PROBLEM

While the e-banking offers enormous advantages and opportunities, it also presents various security risks. With this in mind, banks take extensive steps to protect the information transmitted and processing when banking online. This includes for example, ensuring that confidential data sent over the internet cannot be accessed or modified by unauthorized third parties. But the banks normally have no influence over the systems used by their customers. The choice is entirely up to them. Moreover, the system selected – a PC connected to the internet, for example – will usually be used for a number of other applications as well. The systems used by online banking customers are therefore exposed to risks beyond the banks control. For this reason, the banks cannot assume liability for them. To ensure that the bank's security measures cannot be undermined by manipulation, it is essential that customers, too, follow safety measures. Hence, as it is necessary to analyze the extent of safety measures followed by customers while e-banking, this paper focuses on the precautions to be taken by e-banking customers, their awareness about various e-banking scams and suggests measures for a secured e-banking.

OBJECTIVES OF THE STUDY

1. To study the various services available through online banking
2. To study the various types of online banking scams
3. To study the extent of precautions followed by customers while e-banking
4. To suggest safety measures while e-banking

SIGNIFICANCE OF THE STUDY

A high level of perceived risk is considered to be a barrier to propagation of new innovations in e-banking. Influenced by the imagination – capturing stories of hackers, customers fear that an unauthorized party will gain access to their online account and serious financial implications will follow. "Security" is the biggest single concern for customers when faced with the decision to use internet banking. Security has always been an issue, but its scope has changed from mere doubts about the privacy of personal information to worries of financial loss. Hence, this study measures the extent of safety measures followed by e-banking customers, educates the e-banking customers regarding the various online scams and suggests the safety measures to be followed while e-banking. The study will help bankers to know the safety measures followed by their customers which will enable them to take steps to educate their customers on safety measures while e-banking. The suggestions provided will help the customers to bank safely.

SCOPE OF THE STUDY

This study is premised on the current safety measures followed by customers in e-banking residing in Kalyan City. Therefore, responses of selected respondents are sought in providing answers to the research questions. The focus of the research in terms of study groups includes businessmen, doctors, academicians, bank officials, housewives and engineers who used e-banking facility in Kalyan City. Responses from the study groups were analyzed to measure the extent of safety measures followed by them and suggest them with the required safety measures while e-banking.

RESEARCH DESIGN

Survey research design and secondary data was used in this study. This research strategy was considered necessary because of its ability to view comprehensively and in detail the major questions raised in the study.

STUDY POPULATION

A population is the entire set of relevant units of analysis. Thus, businessmen, doctors, academicians, bank officials, housewives and engineers who used e-banking facility in Kalyan City represent the population of the study.

SAMPLING FRAME AND SAMPLING TECHNIQUE

Customers using e-banking facility in Kalyan City, 50 respondents consisting of 4 businessmen, 3 doctors, 20 academicians, 8 bank officials, 10 housewives and 5 engineers who used e-banking facility were drawn randomly where the respondents were approached for participation in the study.

DATA TYPE AND DATA COLLECTION INSTRUMENT

Primary data and secondary data were collected for the study. The primary data was obtained from the targeted respondents through a carefully constructed questionnaire. The questionnaire was designed to capture the demographic data of the respondents and the extent of safety measures followed by the respondents while e-banking. The questionnaire was constructed using a three-point Likert scale. Secondary data was collected to study the various e-banking products and services, facilities offered in e-banking and various e-banking online scams.

METHOD OF DATA ANALYSIS

The data collected were analyzed using percentages.

TYPES OF PRODUCTS AND SERVICES

1. **Total Branch Automation:** It speeds up bank transactions and reduces error, more customer friendly and flexible and paperless transactions.
2. **Any Branch Banking:** It is a facility for customers to operate their account from any of the same banks network branch. Facilities available are cash withdrawal and cash deposits, account statement, facility to issue multi-city cheques, fund transfer, balance enquiry, purchase of demand drafts, pay order and repayment of loan account.
3. **Demat services:** It offers secure and convenient way to track your securities and investment over a period of time without the hassle of handling physical documents. It provides facility of online trading.
4. **Microfinance:** Microfinance refers to a movement that envisions a world in which low income households have permanent access to a range of high quality financial services to finance their income producing activities, build assets, stabilize consumption and protect against risks.
5. **Plastic money:** Plastic money are an alternative to the cash or standard money which is convenient to carry and is a generic term for all types of bank cards, debit cards, credit cards, smart cards.
6. **Mobile Banking:** In mobile banking, the account can travel with you. One can bank from anywhere, at any time and in any condition or any how using mobile phones. Facilities are balance enquiry, fund transfer, cheque book request etc.

TYPES OF ELECTRONIC SYSTEMS

1. **ATM:** ATM stands for Automated Teller Machine. In simple words, it is 'simple to use self-service solution'. It offers value added services like recharging the mobile, paying the utility bills, mutual fund transactions etc.
2. **RTGS:** RTGS stands for 'Real Time Gross Settlement System'. It is a fund transfer mechanism where transfer of money takes place from one bank to another on a real time or gross basis. This is the fastest possible money transfer system through the banking system. It is primarily for large volume transaction. The time taken for effecting funds transfer from one account to another is normally 2 hours.
3. **FINACLE:** This system provides the holistic and integrated transformation approach, complete with solutions and services. Finacle solution addresses the requirements of retail, corporate and universal banking worldwide like core banking solution, E-banking solution, mobile banking solution, wealth management, CRM requirements etc.

VARIOUS TYPES OF ONLINE BANKING SCAMS

With the range of payments becoming ever greater over the world, everyone needs to be aware of the coherent steps that should be taken to minimize the chances of being an online fraud victim. Being a victim of fraud can cause stress and worry, so taking measures to protect yourself is essential. Some common online banking scams are:

1. **PHISHING:** This is the name given to e-mails that claim to be from your bank or other organizations but are actually sent to you by fraudsters. These e-mails typically urge you to click on a link that takes you to a fake website identical to the one you would expect to see. You are then asked to verify or update your personal information but, by doing so, you are actually giving your information to the fraudster who has created the fake Website. The fraudster then uses the details to access your online bank account and take your money. One easy way to spot phishing e-mails is that they are usually addressed to "Dear valued customer" instead of your name. This is because phishing e-mails are usually sent out at random as the fraudsters only have limited information such as e-mail address. In a similar scheme, called 'Vishing', a person calls you and pretends to be a bank representative seeking to verify account information.
2. **PHARMING:** Pharming is the installation of malicious code on your computer without any acknowledgement on your part. In one type of pharming attack, you open an e-mail, or an e-mail attachment that installs malicious code on your computer. Later, you go to a fake web site that closely resembles your bank or financial institution. Any information you provide during a visit to the fake site is made available to malicious users. Both phishing and pharming share the one characteristic, they are created using technology, but in order to be successful, they require your information. In phishing attacks you have to provide the information or visit links whereas with pharming, you have to open an e-mail, or e-mail attachment, to become a victim. You then visit a fake website and, without your knowledge, provide information that comprises your financial identity.
3. **MALWARE:** Malware (malicious software) is a computer virus that can be installed on your computer without your knowledge. It is capable of monitoring your PC activity, enabling fraudsters to capture your passwords and other personal information. To be a malware victim, you must be tricked into performing actions you would not normally do. You have to install the malware on your computer either by running a program or by visiting a website through e-mail or instant message link. Then, you are requested to send your bank login information. Your financial information will then be at risk only after you perform all these steps. To make sure you do not become a victim of malware, make sure you have up-to-date anti-virus and anti-spyware software installed.
4. **MONEY MULES:** Money mules are people who accept fraudulently obtained money into their account, and then withdraw the money and transfer it overseas to a fraudster. Money mules are often innocent people who have been deceived into helping criminals transfer funds abroad. Criminals offer prospective mules the chance to earn some easy money – concealing the fact that the work is illegal by advertising the job as a "shipping manager" or "sales manager" for an overseas company. However, money mules are liable for presentation and anyone who thinks they may have been deceived by such a scam should contact the police immediately.
5. **IDENTITY FRAUD:** This fraud involves criminals obtaining key pieces of personal information that they use to pretend to be you. Criminals use these personal details to obtain financial services products in your name such as credit cards, loans, state benefits and documents such as driving licenses and passports. Alternatively criminals can use your personal information to gain access to your existing accounts.

RESULTS OF THE EXTENT OF SAFETY MEASURES FOLLOWED BY RESPONDENTS WHILE E-BANKING

Although internet banking is a very common way of accessing your bank account, it is vital to be aware of the ways in which criminals can try to gain access to your account and to learn how to protect yourself and your money. Financial institutions that employ any form of internet banking should have effective and reliable methods of authenticating customers. An effective authentication system is necessary in order to comply with requirements to preserve customer information to prevent money laundering, reduce fraud, restrain identity theft and promote the legal enforceability of their electronic agreements and transactions.

The risks of doing business with unauthorized or incorrectly identified persons in an internet banking environment can result in financial loss and reputation damage through fraud, disclosure of customer information, corruption of data.

TABLE 1: AGE OF THE RESPONDENTS

AGE	Number of respondents	Percentage
Less than 20 years	3	6%
20-30 years	7	14%
30-40 years	20	40%
40-50 years	17	34%
Above 50 years	3	6%
Total	50	100%

TABLE 2: GENDER OF THE RESPONDENTS

Gender	Number of respondents	Percentage
Male	32	64%
Female	18	36%
Total	50	100%

TABLE 3: EDUCATIONAL QUALIFICATION OF THE RESPONDENTS

Qualification	Number of respondents	Percentage
HSC	3	6%
Graduate	26	52%
Post-Graduate	7	14%
Doctorate Degree	2	4%
Professional Degree	12	24%
Total	50	100%

4 businessmen, 3 doctors, 20 academicians, 12 bank officials, 8 housewives and 5 engineers

TABLE 4: JOB PROFILES OF THE RESPONDENTS

Job Profile	Number of respondents	Percentage
Businessmen	4	8%
Doctors	3	6%
Academicians	12	24%
Bank Officials	18	36%
Home makers	8	16%
Engineers	5	10%
Total	50	100%

TABLE 5: FACILITIES USED BY RESPONDENTS IN E-BANKING

Facilities in E-banking	YES		NO	
	No. of Respondents	%age	No. of Respondents	%age
a.) Financial transaction such as account to account transfer, bill payment etc	27	54%	23	46%
b.) Electronic bill display and payments	15	30%	35	70%
c.) Funds transfer between customers	8	16%	42	84%
d.) Financial transactions for sales and purchases	43	86%	7	14%
e.) Loan repayment	2	4%	48	96%
f.) Update of savings account	50	100%	0	0%
g.) Online bank statement status	50	100%	0	0%

TABLE 6: EXTENT OF SAFETY MEASURES FOLLOWED WHILE E-BANKING

Safety measures in E-banking	Sometimes		Always		Never	
	No.	%	No.	%	No.	%
a.)Disabling file & printer sharing in your computer	10	20%	5	10	35	70%
b.)Avoiding installation or running software application from unknown sources	7	14%	6	12%	37	74%
c.)Avoid disclosing or entering of personal data like Date of Boirth, CVV number of the credit card, to unfamiliar websites, e-mails	9	18%	35	70%	6	12%
d.)Avoid accessing online banking or performing financial transactions from public terminals or computers or devices which cannot be trusted	13	26%	4	8%	33	66%
e.)Avoid keeping the computer on without logging out while E-banking	16	32%	25	50%	9	18%
f.)Ensuring that the website you are transacting on starts with 'https://' and not 'http://' where 's' means secure	2	4%	4	8%	44	88%
g.)Looking out for an icon of a padlock at the bottom of the browser	1	2%	3	6%	46	92%
h.)Changing your PIN frequently in 2 months	5	10%	2	4%	43	86%
i.)Not to send credit card or account details via e-mail and phone to anybody	4	8%	1	2%	45	90%
j.) Regularly check the monthly credit card billing statements	2	4%	48	96%	0	0%
k.)Checking the website's private policy and install the latest anti-virus software and firewalls	27	54%	13	26%	10	20%
l.)Signing on the backside of a new credit card and keeping an eye on it during the transaction	2	4%	48	98%	0	0%
m.)Destroy the carbons of the credit card receipts	24	48%	7	14%	19	38%
n.)Taking immediate action in case of loss and theft	0	0%	50	100%	0	0%
o.)Ensuring that the credit card is swiped in your presence and the billed amount has been double checked before signing the payment slip	6	12%	43	86%	1	2%
p.)Accessing the internet banking site directly by entering the official bank URL and not through any site or links in e-mail	5	10%	13	26%	32	64%
q.)Checking the last log-in-date in your net banking account	7	14%	3	6%	40	80%
r.)Using the virtual keyboard provided on bank's website for logging in	7	14%	5	10%	38	76%
s.)Checking your credit rating system from time to time to make sure that nobody has tried to take out a loan in your name	1	2%	2	4%	48	96%
t.)Using a secured broadband connection to prevent others from accessing your broadband connection	11	22%	30	60%	9	18%
u.)To activate a pop-up window blocker	1	2%	3	6%	46	92%
v.)Ensuring that the ATM card, credit card & PIN are not kept together	1	2%	48	96%	1	2%

TABLE 7: FRAUDS AWARE OF BY THE CUSTOMERS IN E-BANKING

Various frauds in E-banking	Yes		No	
	No. of Respondents	%age	No. of Respondents	%age
a.)Phishing	12	24%	38	76%
b.)Pharming	7	14%	43	86%
c.)Money mules	4	8%	46	92%
d.)Malware	8	16%	42	84%
e.)Identity Fraud	6	12%	44	88%
f.)Brand Spoofing	5	10%	45	90%
g.)Cyber-Mugging	3	6%	47	94%
h.)Trojan horses	3	6%	47	94%
i.)Keystroke sniffer	2	4%	48	96%
j.)Salami Slicing	1	2%	49	98%
k.)Skimming	2	4%	48	96%

FINDINGS OF THE STUDY

- Majority of the respondents who used e-banking facility was in the age group of 30-40 years
- Majority of the respondents used e-banking facility for account transfer, bill payment, sales and purchases, update of savings account and online bank statement status.
- Respondents followed basic safety measures while e-banking
- Online safety measures are not followed by majority of the respondents as they are not aware of them.
- Offline safety measures are followed by the respondents to some extent
- Overall safety measures followed by the respondents while e-banking is very low
- Majority of the respondents are not aware of the frauds in e-banking and the security available to control internet threats and challenges.

SUGGESTIONS FOR RESPONDENTS WHILE E-BANKING

To improve the security online, one must follow the following precautions:

GENERAL SAFETY PRECAUTIONS

I. BEFORE BANKING ONLINE

- Make sure your computer has up-to-date anti-virus software and a firewall installed.
- Install anti-spyware software on your machine.
- Download the latest security updates, known as patches for your browser and your operating system. Set your computer to automatically download these updates if possible.
- Ensure your browser is set at its highest level of security notification and monitoring. The safety options are no always activated by default.
- Keep your passwords and PINs secret- do not write them down or tell anyone what they are.

II. WHILST BANKING ONLINE

- Be aware of unsolicited e-mails or phone calls asking you to disclose any personal details or passwords. Your bank or the police would never contact you o ask you to disclose your PIN or your online banking password
- Always access your internet banking site by typing the bank's address into web browser
- Never go to a website from a link in an e-mail and then enter personal details
- The login pages of bank websites are secured through an encryption process, so ensure that there is a locked padlock or unbroken key symbol in your browser window when accessing your bank site. The beginning of the bank's internet address will change from 'http' to 'https' when a secure connection is established.

5. Never leave your computer unattended when logged in to your online account
 6. When making a payment, always double check that you have entered the correct account number and sort code – if you enter incorrect details the payment will go to a different recipient and it may prove difficult to get the money back.
- III. WHEN YOU HAVE FINISHED BANKING ONLINE**
1. Ensure you log off from your online bank account before you shut down, especially if you are accessing your online bank account from a public computer or at an internet café
 2. Check your bank statements regularly and thoroughly. If you notice anything irregular on your account, contact your bank as soon as possible.
- IV. SHOPPING ONLINE SECURELY**
- To minimize the chances of becoming a victim of fraud while shopping online, one should:
1. Be aware that your card details are as valuable as cash in the wrong hands so store your cards securely at all times and try not to let them out of your site
 2. Sign up to “Verified by visa” or “MasterCard Secure Code” whenever you are given the option whilst shopping online. This involves you registering a password with your card company. By signing up, your card will have an additional level of security that will help prevent you from being a victim of online fraud.
 3. Only shop through secure sites. Before submitting card details, ensure that the locked padlock or unbroken key symbol is showing in your browser. (The locked padlock symbol is usually found at the top of the screen if you use Internet Explorer 7 or Firefox 2). The beginning of the online retailer’s internet address will change from ‘http’ or ‘https’ when a connection is secure. In some new browser’s such as Internet Explorer 7 and Firefox 2, the address bar may also turn green to indicate that a site has an additional level of security.
 4. Never disclose your PIN to anyone and never send it over the Internet.
 5. Print out your order and keep copies of the retailer’s terms and conditions, returns policy, delivery conditions, postal address (not a post office box) and phone number (not a mobile number). There may be additional charges such as local taxes and postage, particularly if you are purchasing from abroad. When buying from overseas remember that it may be difficult to roll back if problems arise, but having all the aforementioned information will help your card company take up your case if you subsequently have any difficulties.
 6. Ensure you are fully aware of any payment commitments you are entering into, including whether you are authorizing a single payment or a series of payments.
 7. Consider using a separate credit card specifically for online transactions.

CONCLUSION

E-banking has become a must for people’s daily life due to its ease of access and transaction processing in a timely manner. However, many individuals or organizations are not vigilant enough and do not take appropriate safety precautions whilst online. Consequently, this leads to fraudsters capturing their personal information and performing all sorts of fraudulent transactions on the internet. For this reason, users of e-banking should ensure that they follow secure principles when giving away or accessing sensitive information.

REFERENCES

1. Akinci, S., Aksoy, S. and Atilgan, E. (2004), Adoption of internet banking among sophisticated consumer segments in an advanced developing country, *International Journal of Bank Marketing*, Vol.22 (3), pp. 212-32.
2. Aladwani, M. Adel (2001), Online banking: a field study of drivers, development challenges, and expectations, *International Journal of Information Management*, pp. 213- 225.
3. Amato-McCoy, D. (2005), Creating virtual value, *Bank Systems and Technology*, 1(22).
4. Asher, J. (1999), Small business: Suddenly everyone wants a piece of it, *American Bankers Association. ABA Journal*, 91, (4).
5. Barnes, J.G., Howlett, D. M. (1998), Predictors of equity in relationships between financial services providers and retail customers, *International Journal of Bank Marketing*, Vol.16, pp.15-23.
6. Bauer, H.H., Hammerschmidt, M. and Falk, T. (2005), Measuring the quality of e-banking portals, *International Journal of Bank Marketing*, Vol. 23, No. 2, pp. 153-75.
7. Black, N.J., Lockett, A., Winklhofer, H. and Ennew, C. (2001), The adoption of internet financial services: a qualitative study, *International Journal of Retail & Distribution Management*, Vol.29 (8), pp. 390-398.
8. Calisir F. and Gumussoy, C. A., (2008), Internet banking versus other banking channels: Young consumers’ view, *International Journal of Information Management*, Vol.28, pp. 215-221.
9. Centeno, C. (2004), Adoption of Internet services in the Acceding and Candidate Countries, lessons from the Internet banking case, *Telematics and Informatics*, Vol.21, pp. 293-315 .
10. Chou, D., & Chou, A.Y. (2000), A Guide to the Internet Revolution in Banking, *Information Systems Management*, Vol.17 (2), pp. 51-57.
11. Chung, W. and Paynter, J. (2002), An Evaluation of Internet Banking in New Zealand, In *Proceedings of 35th Hawaii Conference in System Sciences (HICSS 2002)*, IEEE Society Press.
12. Daniel, E. (1999), Provision of electronic banking in the UK and Republic of Ireland, *International Journal of Bank Marketing*, Vol.17(2), pp. 72-82.
13. Durkin, M., Jennings, D., Mulholland G. and Worthington, S. (2008), Key influencers and inhibitors on adoption of the Internet for banking, *Journal of Retailing and Consumer Services*, Vol.15, pp. 348-357.
14. Eriksson, K., Kerem, K., & Nilsson, D. (2008), The adoption of commercial innovations in the former Central and Eastern European markets. The case of internet banking in Estonia”, *International Journal of Bank Marketing*, Vol.26 (3), pp. 154-69.
15. Gerrard, P. and Cunningham, J.B. (2003), The Diffusion of internet banking among Singapore consumers, *The Journal of Bank Marketing*, Vol.21 (1), pp. 16-28.
16. Gerrard, P., Cunningham, J.B. and Devlin, J.F. (2006), Why consumers are not using internet banking: a qualitative study, *Journal of Services Marketing*, Vol.20 (3), pp. 160- 168.
17. Grabner-Kräuter, S., & Faullant, R. (2008), Consumer acceptance of internet banking: the influence of internet trust, *International Journal of bank marketing*, Vol.26 (7), pp. 483-504.
18. Guerrero, M. M., Egea, J. M. O. and Gonzalez, M. V. R. (2007), Application of the latent class regression methodology to the analysis of Internet use for banking transactions in the European Union, *Journal of Business Research*, Vol.60, pp. 137-145.
19. Hamlet, C. (2000), Community banks go online, *American Bankers Association. ABA Journal*, Vol.92 (3).
20. Howcroft, B., Hamilton, R. and Heder, P. (2002), Consumer attitude and the usage and adoption of home-based banking in the United Kingdom, *International Journal of Bank Marketing*, Vol.20 (3), pp. 111-121.
21. Hughes, T. (2001), Market orientation and the response of UK financial services companies to changes in Market conditions as a result e-commerce, *International Journal of Bank Marketing*, Vol.19 No.6, pp. 222-231.
22. Ibrahim, E.E., Joseph, M and Ibeh, K.I.N (2006), Customers’ perception of electronic service delivery in the UK retail banking sector, *International Journal of Bank Marketing*, Vol. 24, No. 7, pp. 475-493.
23. Ilett, D., (2005), Online Bankers to Double by 2010, Retrieved on April 8, 2008, <http://www.silicon.com/financialservices/0,3800010322,39153014,00.htm>.
24. IMRB and IMAI (2006), Internet in India- 2006 (Summary Report of I-Cube, 2006), New Delhi: IMRB International (e-technology Group@IMRB).
25. Kothari, D. (2007), Banks are now just a Click or SMS away, *The Week*, Vol.25, No.48, pp.63-76

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 to supply 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 you have 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

