Awareness concerns of Cyber Security for citizens in Navi Mumbai and Panvel Zone

Prof. Tulshiram Kamble, Dr. Pushpendu Rakshit, Dr. Anoop Sharma

PCCCS, Research Scholar, Singhania University, Rajasthan.
Amity Business School, Mumbai, Amity University, Maharashtra
Research Guide, Singhania University, Rajasthan

Date of Submission: 05-02-2023 Date of Acceptance: 20-02-2023

ABSTRACT:
As per the latest reports of RBI our country has seen almost 1 billion digital transaction. The study conducted by Gotlieb, and Denny [1993]' is one of the studies that deals with the impact of IT on banking productivity per second. Computerization is one of the factors which improves the efficiency of the banking transactions. Respondents were selected on the basis of convenience and data was collected over a span of three months. There is a benefit of having small sample size Malhotra (1999) thus 221 questionnaires were filled for problem solving keeping responses confidential, as it not only provides better average mean values but also avoids errors which may exist in case of large sample.

Through the literature review from multiple dimensions, it gives a clear picture that computer / cyber security or related concerns are historic in nature. It is also used to include traditional crimes in which computers or networks are used to enable the illegal activity. The doctoral study is conducted on the customers of Navi Mumbai and Panvel zone in the city of Mumbai (Maharashtra, India) to find the level of awareness regarding Computer forensics aspects along with further developments in the unexplored field of techno legal skill development, as it is one of the developed financial and commercial cities in modern era.

KEYWORDS: Cybercrime, awareness, financial institutes, cyber-attacks, government acts & laws, security procedures.

I. INTRODUCTION:

Hart in his work “The Concept of Law” has said ‘human beings are vulnerable, so rule of law is required to protect them’. Applying this to the cyberspace we may verbalize that computers are insecure, so rule of law is requisite to protect and safeguard them against cybercrime. The reasons for the vulnerability of computers may be said to be:

1. Capacity to store data in comparatively small space
2. Easy to access
3. Complex
4. Negligence
5. Loss of evidence

The number of individuals victimized by c omputer crimes has increased annually (Gordon, L oef, Lucyshyn, & Richardson, 2004). Flanagan and McMenamin (1992) state computer Crime-committ ed by new generation of hackers might cost cybercr ime victims,as a collective, anywhere from$500mil lion to $5 billion a year. The Computer Emergency Response Team Coordination Center(CERT/CC) re ports that “the number of reported incidences of sec urity breaches in the firms three quarters of 2000 ha s risen by 54% over the total number of reported in cidences in 999”(McConnell International LLC, 20 00, p.1). This Suggests that the hacker world is rapidly changing for the worse. Kabay’a (2001) summary of studies and surveys of computer crime estimated that losses to victims of virus infections reached approximately $ 7.6 billion in the first half of 1999. Moreover according to the 2005 CSI / FBI Computer Crime and Security Survey, virus attacks continue to effectuate the most substantial financial losses and compared to the year 2004, monetary losses have significantly escalated due to “unauthorized access to information” and the “theft of proprietary information” (Gordon et al., 2 004, p. 15). The study conducted by Gotlieb, and Denny [1993]' is one of the studies that deals with the impact of IT on banking productivity per second. Computerization is one of the factors which improves the efficiency of the banking transactions. Navi Mumbai is a developed business hub with many banking and financial institutions providing financial services to customer in both the cities. As per the statistics from RBI report (2014) about Credit card transaction taken place is 4,38,032 via (asynchronous transmission medium) ATM and 5,60,91,791 via point of sales (POS) and amount transacted in millions via ATM is 2505.79 and that via POS 171865.26. Same in case of Debit cards transactions via ATM is 59,10,56,613 and POS is 7,36,18,740 and amount transacted in millions via ATM is 1897693.28 and POS is 111006.57 as per year December 2014.

Credit card transaction taken place is 4,40,618 via (asynchronous transmission medium) ATM and 11,28,02,575 via point of sales (POS) and amount transacted in millions via ATM is 1539.2 and that via POS 327082.5 where as in case of Debit cards transactions via ATM is 71,23,47,249 and POS is 32,86,23,459 and amount transacted in millions via ATM is 1516436.7 and POS is 490041.9 as per year January 2017. Thus, is becomes too important to conduct a study for the same to understand customers perspective towards cyber security awareness post demonetization.

In present scenario the cyber-crimes are increasing day by day. After introducing the cyber law in our country the cyber-crimes[349] are becoming less but now also some of the cases are their which changes the public mind about the people of our country. Through cyber law many people got arrested and they are now also behind the bar. After seeing so much safety the people are not creating much violence about this. Because of cyber-crime many people had being suffered and mainly the rich people and the girls. Therefore Cyber-crime system requirements in India are being increasing day by day as per the crimes are increasing.

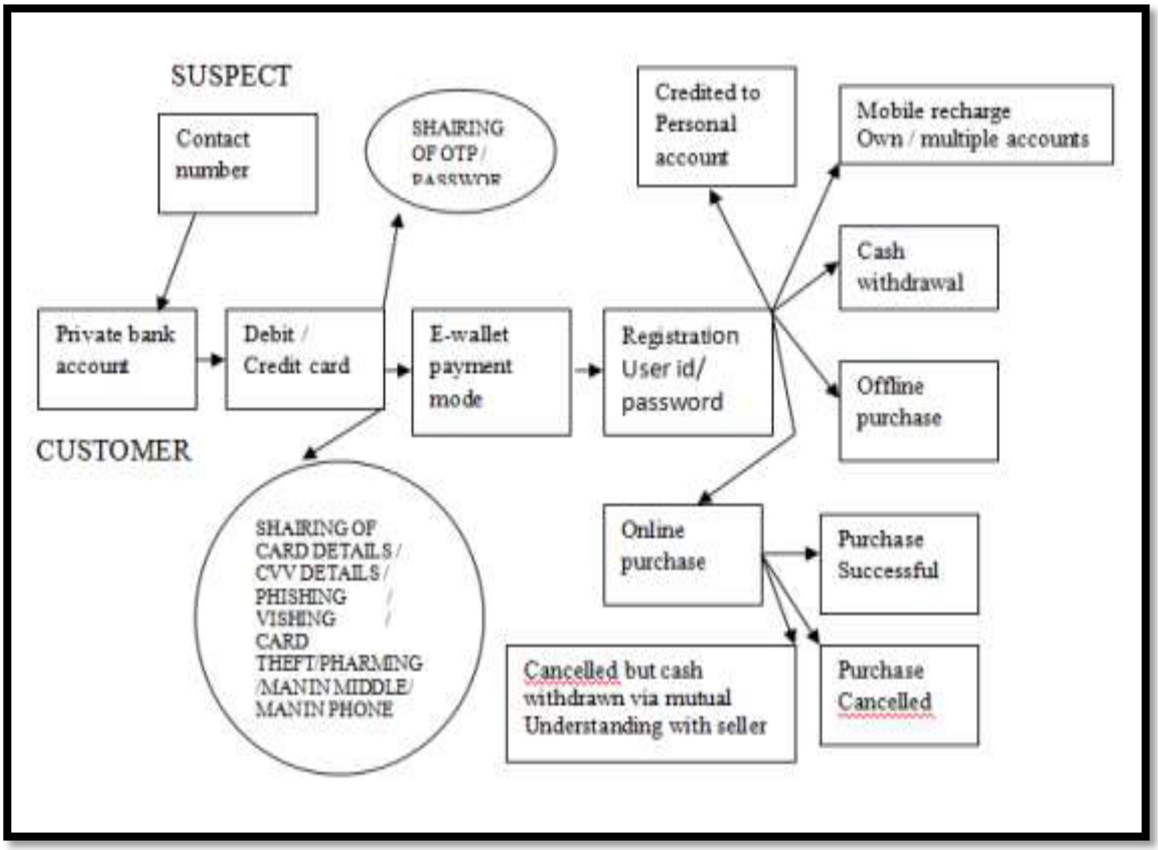
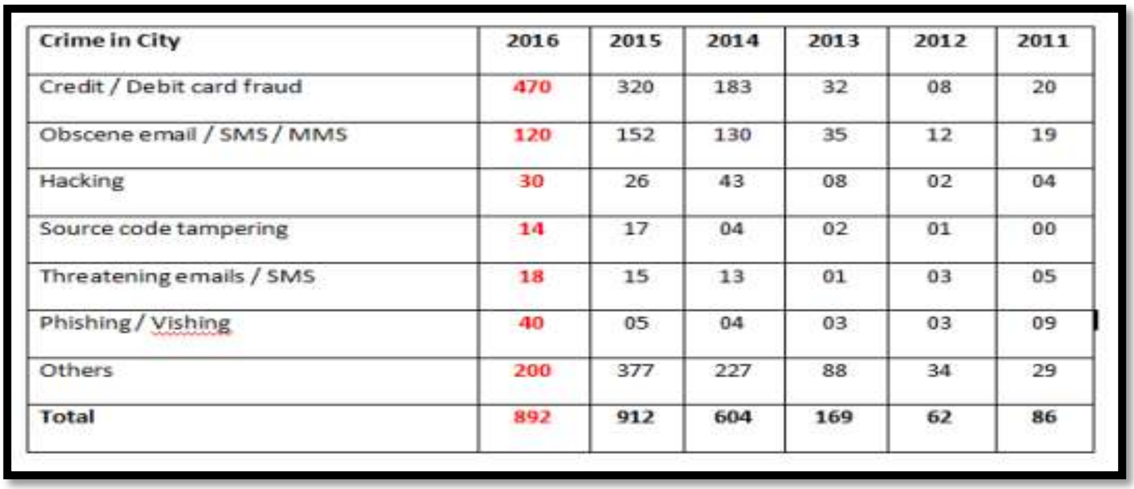

SUSPECT
Contact number
SHAIRING OF OTP / PASSWOR
Credited to Personal account
Mobile recharge Own / multiple accounts
Cash withdrawal
Private bank account
Debit / Credit card
E-wallet payment mode
Registration User id/ password
Offline purchase
CUSTOMER
SHAIRING OF CARD DETAILS / CVV DETAILS / PHISHING / VISHING / CARD THEFT/PHARMING /MANIN MIDDLE/ MANIN PHONE
Online purchase
Purchase Successful
Cancelled but cash withdrawn via mutual Understanding with seller
Purchase Cancelled

Figure 1- Flow diagram of online financial transaction fraud



Crime in City	2016	2015	2014	2013	2012	2011
Credit / Debit card fraud	470	320	183	32	08	20
Obscene email / SMS / MMS	120	152	130	35	12	19
Hacking	30	26	43	08	02	04
Source code tampering	14	17	04	02	01	00
Threatening emails / SMS	18	15	13	01	03	05
Phishing / Vishing	40	05	04	03	03	09
Others	200	377	227	88	34	29
Total	892	912	604	169	62	86

Figure 2- Web Offenses of Navi Mumbai & Panvel Zone

OBJECTIVES FOR THE STUDY:

The objectives of this research work are to touch all the important facets of the cybercrimes in a comprehensive way and to achieve new insights into it.

1. To examine that how cyber security awareness is important for customers while using online / methods of financial transactions?

II. REVIEW OF LITRETURE:

Information Technology (IT) is very powerful in today's world, and financial institutions are the backbone of the Indian economy. Indian Banking Industry today is in the midst of an IT revolution.

Over the past two decades, cybercrime has emerged as a salient area of inquiry for criminologists and a growing concern for public policy. Although there are many definitions of cybercrime, the term generally refers to crimes committed through the use of computers and computer networks, but it also includes crimes that do not rely heavily on computers (Britz, 2008). Extant research has explored the nature and extent of cybercrime (Cukier& Levin, 2009; Finley, 2009; Finn, 2004; Geis et al., 2009; Huang et al., 2009; Jaishankar, Halder, &Ramdoss, 2009; Ponte, 2009; Stroik& Huang, 2009), correlates of offending and victimization (Berg, 2009; Bossler & Holt, 2010; Buzzell et al., 2006; Choi, 2008; Higgins, 2005; 2006; Higgins, Fell & Wilson, 2007; Higgins & Makin, 2004; Higgins, Wolfe & Marcum, 2008; Holt & Bossler, 2009; Marcum, 2008; Skinner &Fream, 1997; Turgeman-Goldschmidt, 2009) and issues relating to investigating and prosecuting this type of crime (Roberson, 2009; Hinduja, 2009; Shoemaker & Kennedy, 2009). In spite of the considerable and growing scholarship on cybercrime, however, few studies have examined the theoretical causes and correlates of cybercrime victimization.

RESEARCH DESIGN:

- Deductive Approach (Qualitative)
- Testing theory through observation and data (Primary & secondary).
- Exploratory Study
- Purposive, (deliberate) self-selection sampling and area sampling.
- Longitudinal
- Projects must be around 1 year in length.
- Collection of data
- In- depth personal interview at beginning with banks and cyber cell.
- Questionnaire method.
- Delphi method / expert advice for probable solutions
- Self-completion diaries
- To track issues and dynamism in cyber space.
- Sample size - 221

PROBLEM FORMULATION:

There has been no comprehensive study in the areas of the impact of cyber security issues in the banks (Clarke &Knake, 2010) of Navi Mumbai and Panvel zone, at best there has been a reference made to attacks with mitigation and prevention, general customer satisfaction for services and intrusion detection.

There has been no complete list or in-depth description of cyber security measurements and customer's perspective followed by the banks. There have been studies that took at one aspect of banking cyber securities and fraud detection or prevention techniques but had a lacuna to further enhance the banking system security that holds customer information and large amount of finance. Also, to mention that studies were still not conducted on the local branches of banks in localities for the research. Thus, there is a gap this research aims to fulfill.

III. FINDING, DATAINTERPRETATIONAND ANALYSIS:

The proportion of male is 33% and female is 67% among respondents.

The sample respondent was skewed towards population aged between 19-24 years (90%). About 7.2% belonged to the age group of 25-34,0.5% for 35-44, 1.4% for 45-54, 0.5% for 55-64 and 0.5% for 65+.

The sample respondent had population of 93.2 % for bachelor's, 2.7 % masters,0.5% doctoral,1.4% high school, 1.4% associate and 0.5 % others.

About 53.4% were found using computer / internet for 3-5 hours a day whereas 24.9% uses for 6-8 hours, 17.6% uses for 0-2 hours and 4.1% for 12+.

About 75.6% have moderate knowledge of internet technologies, 16.3% have high, 5.4% have low and 2.7% has expert.

About 44.3% are found very familiar whereas 49.8% are somewhat familiar.

It was found that about 31% thought that the Bandhan Bank was most vulnerable to cyber frauds whereas 19.5% said Axis Bank, 16.7% said ICICI Bank, 11.8% said City Bank, 10.4% said City Union Bank and only 10 % said HDFC for the perspective zones in the study.

Statistics says that about 28.5% customer were victims of credit / debit card frauds whereas 24.9% for electronic / e wallet fraud, 21.9% for ATM fraud, 12.7% for phishing / vishing and that of about 12.2% for identity theft in the study.

The study reveals that Phishing with 42.5% stands for most known cyber attacking technique Credit / Debit card frauds whereas 29.9% for password stealing, 24.9% vishing and 4.8% for loss of cards.

Study further states that around 24.4% sample space claims demonetization as a reason for increase in cybercrimes in Navi Mumbai and Panvel Zones in the current scenario.

The study reveals that around 72.9% of sample space states that banks does not provide alerts and conducts awareness programs for cyber security aspects in current scenario and only 27.1% says yes for the same. As it is understood that most of the crowd are not cyber illiterate and only alerts via simple messing system (SMS) may not be that much accurate and many even fail to have electronic mail accounts.

81% of sample size uses e wallet / online money transfer applications post demonetization whereas only 19 % still moves with conventional methods.

91% says that they have never been participated in any of such awareness campaigns related to cyber security conducted by banks and its only 9% that have been there for same.

About 65.2 % customer receives mobile alerts from banks whereas 19% via electronic mails, 12.2 % via advertisements and around 8% receives physical copy for the same.

In case of customer becoming a victim of cybercrime around 67.9% customers tends to block their cards, 11.8% sets up investigation, 8.6 % ask banks to hold for further transactions and very few land up lodging complaint against the same to cyber cell / police station.

It is also found that around 58.4% are still unaware about the legal rights and the cyber laws for protection against cybercrime, whereas 41.6% says they possess understanding for the same.

53.8% of sample size are partially aware of the procedure to lodge a complaint to banks / cyber cell / police department / other authorities, whereas 18.6 % are interested to know, 11.3% are somehow fully aware and 16.3% still unaware for the same showing importance of cyber know how in current scenario.

56.1% of sample space said these kinds of survey / seminars / workshops would create awareness among respondents regarding cyber frauds / security measures.

DELPHI METHOD OUTCOMES

Expert's adviceis always an important part of the study. The expert advicewas taken from group holding Bankers, Cyber lawyers, Cyber cell experts and solution providers to the financial institutions. All the recommendations are consolidated throughout the study as and when needed. Thus, the study has been giving practical exposure towards the realistic gaps and real time solutions for the same.

Below are the activities advised to the Bank which they must follows to prevent from cyber-attacks:-

- Setting up of NOC-SOC (network operations center- System on a chip) enabling BANK to effectively detect and protect against security threats, which amongst other areas inter-alia cover the following area of operations: Continuous Incident Monitoring and Management Process to address the identification and classification of incidents, reporting, escalation, preservation of evidence and the investigation process for critical systems like Firewalls, Routers, Switches, Servers, Operating Systems, Storage, Databases and Applications like Portal, Website, Email & other components like IP Telephony communication infrastructure, etc. through SIEM(Security Information and Event Management) solution. Also, to provide & integrate various security tools like Vulnerability Assessment Tool, Network Behavior Analysis Tool and Database Security Tool with Security Information and Event Management (SIEM) solution.

- To provide various solutions/ services like Enhanced Security, Risk Management, Vulnerability Management, Governance, Risk and Compliance (GRC), Incident Response, countermeasure Planning, Anti-Phishing, Anti-Malware, Anti-Trojan, Network Level Data Loss Prevention (DLP), prevention from Advance persistence Threats (APT) ,Security Device Management and Administration as a part of SOC-NOC.
- To implement security solutions such as Intrusion Prevention Systems(IPS), Web content filters, Web Application Firewall (WAF) ,Anti-APT solutions, Sandboxing, Mobile Device Management (MDM), virtual browsing solutions

Below is the scope includes all the activities related to information security which can form part of a Network and Security Operations Centre (NOC-SOC) including anti-phishing, anti-malware, anti- Trojan , Anti-Ransom and implementation of security solutions such as IPS, Web content filter, WAF and Anti-APT ,DLP, sandboxing, MDM ,virtual browsing solutions at BANK. The proposed NOC-SOC and security solutions would cover all IT assets of the Bank (including Regional offices and Local offices)

1. To build a well-functioning Network-Security Operations centre (NOC-SOC) which can enable BANK to effectively detect and protect against security threats. Enable information security functions to respond faster, work more collaboratively and share knowledge more effectively.
2. NOC-SOC to be equipped with broad range of capabilities with a diversity of experiences (eg: incident responders, IPS, analysts, knowledgeable forensic analysts with proper network experience).
3. NOC, SOC and other security solutions to work in collaboration so that improved communication and shared knowledge will enhance situational awareness and response capabilities. Improve countermeasure planning through joint accountability for identification and resolution of root cause. Stream-line incident management reporting with valuable technical context.
4. NOC-SOC to document and communicate processes effectively and implement change management mechanisms to quickly update processes when improvement opportunities arise. SOC also needs to create processes with enough breadth and depth to sufficiently address the universe of possible incident scenarios and provide detailed guidelines for response, for example; a SOC must document processes to sort various types of incidents (e.g. phishing, malware infections, BYOD (Bring your own devices) related incidents, website defacement, denial-of-service attacks, etc) as well as decision guidelines for the appropriate response measures for each (e.g. deployment of incident response team, forensic investigation, malware analysis) . NOC-SOC will need to define and implement these processes in collaboration with related departments.
5. NOC-SOC to be equipped with a suite of technology products. Some of the required tools may include intrusion detection and prevention technology(IPS), Anti-APT ,WAF ,web content filter ; SIEM solution; threat and vulnerability management tools; Advance Anti Malware , Anti-Ransom ware tools; filtering technologies; data loss prevention tools; traffic/inspection solutions; data analytics platforms and reporting technologies. In addition, depending on the scope of the responsibilities, the SOC may also have access to other business systems such as enterprise forensic tools in support of incident response investigation efforts. Technologies available in house may also be used to meet SOC needs. Analytics can be used to create more insightful metrics and performance measures to facilitate operational measurements and make informed decisions.

IV. CONCLUSION:

The contribution of this study is also relevant as an eye opener for both customers as well as financial institutions. The study can facilitate the designing and driving of more effective cyber security protective measures and processes and further studies can be useful for all. Thus, security concerns can be provided a bettersolutions. Through the questionnaire the customers could attempt to close the gap between what they perceive as relevant to ethics and the extent to which they are practiced. Also, it could evoke interest in practices which are not yet considered mandatory but could be learnt from this study in the near future.

This analysis is the first of its kind to establish a clear, comprehensive and empirical evidence that emphasis to customer awareness from security perspective is profitable and good business investment. First time a workable list of customer awareness and perspective regarding cyber security and their satisfaction level for the same is established, tested and validate the need to follow such practices in the location selected for the study. Being a commercial hub the probability of acceptance of the same is more.

REFERENCES:

Bibliography - Section 2: Printed Publications and articles

[1]. Arora K. (2003), 'Indian Banking: Managing Transformation through IT', IBA Bulletin, Volume 25(3), March, pp 134-38

[2]. An Investigation of Financial Fraud in Online Banking and Card Payment Systems in the UK and China by Yan Sun, Loughborough University May 2010.

[3]. Adv B Gordon Computer Crime – An Introduction (2002) February Servamus 35.

[4]. Ahmad, Tabrez, New Begining of Cyberlaw in India (July 29, 2009). Available at SSRN.

[5]. After Websites, Anonymous India to Hit Streets Against Cyber Laws,By Manoj Kumar. International Business Times, June 9, 2012.

[6]. AshishPande, Deviation and Prevention, 2006, p. 126.

[7]. An Explorative Study of Satisfaction Level of Cyber-Crime Victims with Respect to E-Services of BanksJournal of Internet Banking and Commerce, Vol. 17, No. 3, 2012 Dr.AtulBamrara ,Gajendra Singh Chouhan ,Mamta Bhatt.

[8]. Bharti, Dr. Dalbir, Police and People – Role and Responsibilities, APH Publishing Corporation, New Delhi, 2006.

[9]. Bayley, David H., "Community Policing", SardarVallabhbhai Patel Memorial Lectures (1984-2004), SVP National Police Academy, Hyderabad, 2005.

[10]. Brynjolfsson Erik (1993) "The Productivity Paradox of Information Technology", Communication of ACM, Vol. 36(12),p.67-77.

[11]. Brynjolfsson, Erik, Hitt, Lorin (1996) "Paradox lost? Firm-level Evidence on the Returns to Information Systems Spending", Management Science, April, Vol.42 No.4, p.541-558.

[12]. Business Standard, Mumbai Police fall prey to cyber crime, Salary accounts with AXIS bankhacked, Sanjay Jog & Krishna Pophale | Mumbai June 14, 2013.

[13]. Byte by Byte, cybercrime.planetindia.net, Gopika Vaidya-Kapoor, The Cyber Regulations Appellate Tribunal, February 18, 2003.

[14]. Chopra V. K. (2006), 'IT and Business Process Re-Engineering', Indian Bankers –Special Issue on e-payments and Commerce, Volume 1(3), March.

[15]. Chakravarthy, S.K., "Social Acceptability of the Police", The Indian Police Journal, Vol. XXVI, No. 1, July-September, 1979, p.3.

[16]. Christopher D Chen Computer Crime and the Computer Fraud and Abuse Act of 1986 (1990) Computer Law Journal Vol. X No. 1 79.

[17]. Choudhary, J.N., "Indian Police Leadership – Can it meet the Challenges of 21st Century", SVP National Police Academy Journal, Vol. 52: No. 2, July-December 2000.

[18]. "China blames US and India for Cyber Attacks", The Hindu, August 11, 2011, p.20

[19]. "Cyberabad Police to Roll out Host of New Measures", Staff Reporter, The Hindu,January 02, 2009.

[20]. Centre Of Excellence For Cyber Security Research And Development In India (CECSRDI), Cyber Security Research And Development Centre Of India (CSRDCI) ,May 10, 2013.

[21]. Cyber laws: Loopholes aplenty, PriyankaJoshi,Business Standard, Mumbai November 18, 2011. [40]

[22]. Cybercrime now 'number one' threat: Europol chief,Agence France-Presse , 20 April 2015, Indian Cyber Crime Centre.

[23]. CyberLawIndia.Net.

[24]. The Menace of Cyber Crime, Anusuya Sadhu, http://www.legalserviceindia.com/articles/article 2302682a.htm.

[25]. Offences & Penalties under the Information Technology Act, 2000,PradnyaPahurkar,LawProfessor,November 17, 2010.

[26]. Police minister announces plan to combat cyber-crime, eyewitness news, shamiela fisher , 2014.
[27]. Reliance Capital files complaint against fake website, Press Trust Of India , 3 June 2013.
[28]. Reserve Bank of India. (1984). Report of the Committee on Mechanisation in Banking Industry.