ISSN 2349-7807

International Journal of Recent Research in Commerce Economics and Management (IJRRCEM)
Vol. 2, Issue 2, pp: (48-56), Month: April 2015 - June 2015, Available at: www.paperpublications.org

Safety Mechanism of Cyber Crime in Indian Banking System

[1]Dr. Sanjeev Mehrotra, [2]Pooja Pasricha

[1]Associate professor and Head, faculty of commerce, Govt. P.G College, Ramnagar, Nainital (Uttrakhand) , India
[2](Research Scholar), Department of commerce, Govt. P.G College, Ramnagar, Nainital (Uttrakhand), india

Abstract: **Use of technology in financial services of course has given a tremendous impetus to their development however, due to heavy dependency on electronic and digital tools to carry out business and payment transactions, a serious threat has also been imposed to the safety and reliability of financial operations. This technology word changes the human life in every manner and every sector. Banking field is one of them. Banking in India originated in the last decades in 18th century. Since that time banking sector applying different ways to provide facilities and securities to a common man regarding to money. Security issues play extremely important role in the implementation of technologies specially in banking. The banking sector is at the core of who comes to cyber security becomes more important on that front. After the arrival of internet and world wibe web communicating banking sector is totally change specially in terms of security because now money is in your hand on a single click, Now users with different kinds of ways is the number of options to manage your money. In this paper an attempt to cyber security mechanism put forward an issues of Indians banks websites.**

Keywords: **mechanism, cyber security, communicating banking sector, banking sector.**

1. INTRODUCTION

The reserve bank said there was an attempt to hack the web site on 24-5-2012 Thursday, rendering it in accessible for almost the entire day. "It was a DNS (Domain Name System) attack where the hacker tried entering the website from a single internet protocol address multiple times, jamming its bandwidth" an RBI spoken person said. Due to multiple request received from the hacker's IP address. Its unable to access the RBI website – www.rbi.org.in.

"We found the IP address and blocked it and got the website on its feet again," the spokesperson said, adding there was no loss of information or defacing as the hackers could not get into the site. For more Details like the exact time period when the hacking happened and the geographical location where the attack has been traced to, are still unclear. A senior official with the Mumbai Police's cyber crime investigation cell said it has not received any complaint from the RBI regarding the incident, but in one of the tweet anonymous hacking group taken the responsibly of this attach. Anonymous is a biggest hacker group in the world they did not agree with move of government, their demand is do not censer internet by making law. They are protesting against the censorship of internet

Banking is the one of the oldest professions to mankind. It has undergone many a transition and internet banking is the latest in the list of such transformations. Internet banking has brought about a 360 degree change in the entire banking industry. Such in the change in scenario that timing is no longer a constraint and you can finish your day-today chores and bank leisurely when you have the time i.e. 24x7 services. Current situation shows that the Internet banking users are prown to such issues and the data shows that in general, only about 20% users of Government public sector Banks like SBI, Bank of Baroda and Punjab National Bank are using net banking while 50% users of private sector Banks like ICICI, HDFC are using net banking. This data clearly indicates that the chances of such crimes are quite possible with private sector banks.

The world of internet today has become a parallel form of life and living. Public are now capable of doing things which are not imaginable few years ago. The internet is fast becoming a way of millions of people and also a way of living

because of growing dependence and reliance of mankind on these machines. Internet has enabled the use of website communication email and lot of anytime any where IT solutions for the betterment of human kind. Today emails and websites have become the preferred means of communication. Organizations provide access to their staff. By their very nature they facilitate almost instant exchange and dissemination of data, images and variety of material. This includes not only educational and informative material but also information that might be undesirable or anti social.

Regular stories featured in the media on computer crime includes topics covering hacking to viruses, Web-jackers, to internet pedophiles, sometimes accurately portraying events, sometimes misconceiving the role of technology in such activities.

Defending a computer system against malicious attack depends on making many different cracy mechanisms work together. In addition to protecting against instructions, there mechanisms should provide intrusion detection and response. The semantics of input and output of these mechanisms –What the alert from an intrusion detector means, and the implications of issuing a command in response can vary greatly from one mechanism to another.

Today, organisation information systems and networks are vulnerable to attack by both insiders and outsiders. Organisations cannot conduct business and build products without a robust IT infrastructure. In addition, users have an organizational and ethical responsibility to protect competitive and sensitive information. They must also preserve the reputation and image of their organizations and business partners. All of these can be severely compromised by successful intrusions.Thus there is a need for a robust information security system to be in place in every organisation.[1]

Information security has the objective of preserving confidentiality, integrity and availability of information in an organisation and is achieved by combining good components, good architectural design, and good practices for the computerized operations.[2]

Security cannot be purchased. It involves effective processing of various components. That is similar to maintaining security of a home against burglary; strong and reliable door locks (components) cannot be effective unless everyone in the house remembers to lock them properly (process). Checking all doors and windows before leaving on vacation (process) will not prevent a burglar from breaking in if one of the windows has flimsy locking mechanism (a single weak component can break the security of the system).[3]

In practical terms, a security policy is a published setoff documents laying out the organisation's philosophy, strategy, policies, and practices with regard to confidentiality, integrity and availability of information and information system.[4]

Phishing is a way of attempting to acquire sensitive information such as usernames, passwords and credit card detail by illegally as a trust worthy entity in an electronic communication. Communications purporting to be from popular social websites, auction sites, online payment processors or IT administrators are commonly used to lure the unsuspecting public. Just it can say that phishing is one type of many frauds. On the internet, trying to fool people into parting with their money. Phishing refers to the receipt of unsought emails by customers of financial institutions, asked them to enter their username, password on other personal information to access their account for some reason. Customers are directed to a website which could be fraud copy of the original institutions websites. When they click on the link on the email of enter their informations, and so they remain unaware that the fraud has occurred. The criminal than has access to the customer's online bank account and to the funds contained in that account number.

[1] MACMILLAN, Security In Electronic Banking, Macmillan Publishers India Limited., Page No- 5 , Paragraph no-3 Publishing Year 2007.
[2] MACMILLAN, Security In Electronic Banking, Macmillan Publishers India Limited., Page No- 5 , Paragraph no-4 Publishing Year 2007.

[3] MACMILLAN, Security In Electronic Banking, Macmillan Publishers India Limited., Page No- 5 , Paragraph no-5 Publishing Year 2007.
[4] MACMILLAN, Security In Electronic Banking, Macmillan Publishers India Limited., Page No- 5 , Paragraph no-6 Publishing Year 2007.

2. CASE RELATED TO PHISING

An email allegedly from Indian central bank, asking to secure their bank account details with the RBI is fake, and an attempt by new-age fraudsters to can people into giving away bank account details and lose hard- earned money, security experts said.

The e-mail say RBI has launched a new security system, asking users to click on a link to open a page with list of banks in place. Once anyone choose a particular bank it ask for all net banking details, including card numbers and the secret three digit cvv number, among others. "The email is so neat and I for once was thrilled that RBI is taking such a big step to ensure the security of people. But at the advice of the friend, Mr. X checked with police and learned that he would lost all his saving to this racket.

RBI is cautioning people that the central bank, which controls the monetary policy of the Indian rupee, has not developed any such software and nor has it sent any such mail asking on line banking customers to update their account details to secure their online accounts. The RBI does not even have any mail Id with extension @ rbi.com, the central bank says.

3. OBJECTIVES OF THE STUDY

The present study objectives:-

1) To determine the issues of effectiveness and secureness banking.

2) To describes cyber crime cracy mechanism for banking Industries.

3) To indentify the status of Indians banks.

4. INTERNET BANKING SECURITY CONTROLS AND MEASURES

According to RBI report, security of online banking transactions is one of the most important areas of concerns to the regulators. Security issues include questions of adopting internationally accepted state-of-the art minimum technology standards for access control, encryption / decryption (minimum key length etc), firewalls, verification of digital signature, Public Key Infrastructure (PKI) etc. The regulator is equally concerned about the security policy for the banking industry, security awareness and education. So the information systems security could be achieved by implementing a suitable set of controls which consists of policies, practices, procedures, organisational structures, hardware and software functions. Each organisation has to establish these controls to ensure that its security requirements are met.

4.1 Information Security Policy (IT vision of reserve Bank India)

Information Security Policy is a documented business rule for protecting information and the systems which store and process this information. Within an organization, the written policy document provides a high-level description of the various controls the organization will use to protect information. The strength of any system is no greater than its weakest link. Information should be based on the principles of integrity, reliability, and validity. Protecting confidential information is a business and legal requirement. The existing IS policy would have to be reviewed and updated at periodical intervals. The IS Policy may detail principles for protecting information from unauthorized access, use, disclosure, disruption, modification or destruction. The information security policy should, inter alia, relate to policies such as firewall, email, network security, and password. The policy should also address issues relating to prevention of cyber attacks by deploying appropriate technologies such as two-factor authentication. Structured, well defined and documented security policies, standards and guidelines lay the foundation for good information systems security and are the need of the hour. The Board of Directors/Management of each organization has the responsibility for ensuring appropriate corporate policies, which set out the management responsibilities and the control practices for all the areas of information processing activities. A well-defined corporate security policy has to be put in place and periodically reviewed and amended, as required, under the approval of the Board of Directors/Management.

4.2 Security Systems (Hardware and Software)

Numerous transactions are carried out on a daily basis hence it's necessary for the bank to have proper security systems that secure its assets from internal and external threats. Some of the measures taken by banks are:

- Firewalls, intrusion detection systems, Switches, anti-virus as well as routers to secure the perimeter..
- Application security is reviewed periodically, every application undergoes an assessment before implementation in production
- Encryption for desktops and laptops to secure data being carried out on media.
- Biometrics was implemented for critical departments. This has helped reduce user ID and password sharing.
- The bank has a desktop management suite which helps the IT team scan the environment for deviations and take corrective action. This helps identify discrepancies and violations of security policy, check for spyware and adware, block device ports (USB, Infrared, Bluetooth) from a central console and check for policy non-compliance on servers. Using the software they also conduct vulnerability Assessment (VA) and patch management on desktops and servers to keep them updated with the latest security patches, helping to reduce risks involved with insecure systems being exploited.
- The bank uses standard messaging software that eliminate the risk of using free software which provides various features other than messaging and may be detrimental to the bank‘s security.

Current Implementation of Security

Mechanisms of Domestic Personal Internet Banking

Type of security measure	**Implemented or not**
SSL encrypted transmission	Yes
CA certificate of the website	Yes
Client certificate	No
Security information authentication	Yes
Shielding Phishing Websites	No
Account protection and reminder	Yes
Double passwords control(Auth. With something the user knows	Yes
Card (Auth. With something the user have)	Yes
One Time Password	Yes
Dynamic password card	No
Virtual keyboard	Yes
Password strength	Yes
The replacement policy	Yes
Active X control	Yes
Automatic overtime	Yes
Mechanism to freeze the incorrect password	Yes
Graphic verification code	Yes

The amount of transactions control	Yes
Account information notification via SMS	Yes
Firewall	Yes
Intrusion detection systems	Yes
Session Timeouts	Yes
Automatic Lock outs	Yes
Expiry of user ID	Yes (After one year)

When you use the internet, your browser (for example Internet Explorer, Opera, Chrome, Safari or Firefox) keeps a record of which sites you have visted in its 'history'.When you use the internet, the websites you visit are visible to your Internet Service Provider and browser provider, and it is possible that records are kept.In order to provide effective and secure banking transactions, there are four technology issues needed to be resolved. The key areas are:

- **Defensive**:- Security of the transactions is the primary concern of the Internet-based industries. In the absence of security, such as the example illustrated in the first section Citibank may cause serious damage. Next to the issue of security attacks due to inadequate safety will be discussed in the next section. The examples of potential hazards of the electronic banking system are during on-line transactions, transferring funds, and minting electric currency, etc.
- **Privacy**:- Privacy issues generally, speaking a subset of the security issue and thus will be discussed in a later section of privacy technology. By strengthening privacy technology, to ensure the privacy of personal information of the sender and will further enhance the security of transactions. Examples of personal information relating to the banking industry: transaction amount, date and time of the transaction, and the transaction is the name of the trader.
- **Certification:-** Encryption may help make transactions more secure, but there is a need to guarantee transaction no change on either end of that data. To verify the integrity of the message are two possible ways. Is a form of verification that is secure hash algorithm "that protects data against the amendment an investigation." Senders transmit data generated hash algorithm. If the two results are different, a change has occurred in the message. The other form of verification is through a third party called Certification Authority (CA) with the trust of both the sender and the receiver to verify that the electronic currency or the digital signature that they received is real.
- **Severability:** Electronic money exchange similar to real money that can be divided into different units. For example, electronic money and money is needed to account for nickels.

5. CYBER CRIME SAFETY MECHANISM

Cyber criminals are no different than traditional criminals in that they want to make their money as quickly and easily as possible. Cyber crime is a term used to broadly describe criminal activity in which computer or computer network are a tool, a target, or a place of criminal activity and include everything from electronic cracking to denial of service attacks.

Criminals are increasingly utilising a variety of technical communication methods for the facilitation of offences and also for the purpose of criminal communications. Tracing the source of communications is essential to discovering offender identity and as intelligence. These communications may be made via ISPs in any part of the world. If any jurisdiction makes it more difficult for law enforcement to obtain details of information, such as subscriber information, then investigations and possible prosecutions will potentially falter.

Cyber criminals will use software flaws to attack computer system frequently and anonymously. Most windows bared systems can be configured to download software patches and updates automatically. By doing this, cyber criminals who exploit flaws in software package may be thwarted. This will also deter a number of automated and simple attack a criminals use to break into your system.

It is important that computer to configured to the security level that is appropriate and comfortable for the user. Too much security can have adverse effect of frustrating the user and possibly preventing them from accessing certain web content.

With the development of the security technology and mechanism of the internet banking, as well as the gradual improvement of the security solutions of the internet banking systems, the internet banking is become more secure. All types of banks in India whether public, private or foreign bank.

When armed with a little technical advice and common sense, many cyber attacks can be avoided. The following are the ways that cyber crime can be prevented.

1) Secure Log-in ID and Password or PIN

- Do not disclose Log-in and Password or PIN.
- Do not store Log-in and Password or Pin on the computer.
- Regularly change password or PIN and avoid using easy-to-guess passwords such as names or birthdays. Password should be a combination of characters (uppercase and lowercase) and numbers and should be at least 6 digits in length.

2) Keep personal information private.

Do not disclose personal information such as address, mother's maiden name, telephone number, social security number, GSIS number, bank account number or e-mail address – unless the one collecting the information is reliable and trustworthy.

3) Keep records of online transactions.

- Regularly check transaction history details and statements to make sure that there are no unauthorized transactions.
- Review and reconcile monthly credit card and bank statements for any errors or unauthorized transactions promptly and thoroughly.
- Check e-mail for contacts by merchants with whom one is doing business. Merchants may send important information about transaction histories.
- Immediately notify the bank if there are unauthorized entries or transactions in the account.

4) Check for the right and secure website

- Before doing any online transactions or sending personal information, make sure that correct website has been accessed. Beware of bogus or "look alike" websites which are designed to deceive consumers.
- Check if the website is "secure" by checking the Universal Resource Locators (URLs) which should begin with "https" and closed padlock icon on the status bar in the browser is displayed. To confirm authenticity of the site, double-click on the lock icon to display security certificate information of the site.
- Always enter the URL of the website directly into the web browser. Avoid being re-directed to the website, or hyperlink to it from a website that may not be as secure.
- If possible, use software that encrypts or scrambles the information when sending sensitive information or performing e-banking transactions online.

5) Protect personal computer from hackers, viruses and malicious programs

- Install a personal firewall and a reputable anti-virus program to protect personal computer from virus attacks or malicious programs.
- Ensure that the anti-virus program is updated and runs at all times.
- Always keep the operating system and the web browser updated with the latest security patches, in order to protect against weaknesses or vulnerabilities.
- Always check with an updated anti-virus program when downloading a program or opening an attachment to ensure that it does not contain any virus.

- Install updated scanner softwares to detect and eliminate malicious programs capable of capturing personal or financial information online.
- Never download any file or software from sites or sources, which are not familiar or hyperlinks sent by strangers. Opening such files could expose the system to a computer virus that could hijack personal information, including password or PIN.

6) Do not leave computer unattended when logged-in

- Log-off from the internet banking site when computer is unattended, even if it is for a short while.
- Always remember to log-off when e-banking transactions have been completed.
- Clear the memory cache and transaction history after logging-out from the website to remove account information. This would avoid incidents of the stored information being retrieved by unwanted parties.

7) Check the site's privacy policy and disclosures

- Read and understand website disclosures specifically on refund, shipping account debit/credit policies and other bank terms and conditions.
- Before providing any personal financial information to a website, determine how the information will be used or shared with others.
- Check the site's statements about the security provided for the information divulged.
- Some websites' disclosure are easier to find than others - look at the bottom of the home page, on order forms or in the "About" or "FAQs" section of a sites. If the customer is not comfortable with the policy, consider doing business elsewhere.

8) Other internet security measures:

- Do not send any personal information particularly password or PIN via ordinary e-mail.
- Do no open other browser windows while banking online.
- Avoid using shared or public personal computer in conducting e-banking transactions.
- Disable the "file and the printer sharing" feature on the operating system if conducting banking transactions online.
- Contacts the banking institution to discuss security concerns and remedies to any online e-banking account issues.

6. STATUS OF DIFFERENT BANK WEBSITES

In this paper we take six Indian banks and try to find out the security features using by the bank for online transactions. The data is collected by various reports from web, newspaper and media. For every security feature we have five points. The banks are:-

- State Bank Of India
- Punjab National Bank
- Bank Of Baroda
- ICICI Bank
- IDBI Bank
- HDFC Bank

Table.1 Point Table

Bank	P.E *	V.K*	SSL*	SMS*	UAP*	TOTAL
SBI	4	4	4	3	3	18
PNB	4	4	3	4	2	17
BOB	4	4	3	2	2	15
ICICI	4	4	3	4	3	18
IDBI	4	4	4	4	2	18
HDFC	4	4	3	4	2	17

*Password Encryption, *Virtual Keyboard, *Secure Socket Layer,*Short message service alerts,*Users Awareness Program.

The study for all of us, being implemented as equal banks found their websites. Encryption virtual keyboard with the password. The banks are safe use SMS Alerts and socket layer information in respect of facilities to provide customers money transaction. We provide 5 marks for each feature but no bank got full 5 mark for any feature and the aggregate total of every bank is vary 15 to 18 out of 25

Reasons for Cracking and Responsibilities:

The reason behind this is that they all have little bit loop wholes on all the security features but the biggest reason are:-

- User Awareness Features
- Negligence
- Lack Of Knowledge
- Complexity of codes
- Improper Language to teach

7. SUGGESTIONS

- What is the meaning of using virtual keyboard
- What is the meaning of strong password
- What is the meaning of SMS alerts
- Don't access net banking account from cyber café or public computer.
- Use a single computer as far as possible.
- Login net banking site by directly typing site name. Don't click any link, if that link takes you to login page, close the page, and start over.
- Bank or its representative never asks for password and username over telephone.
- Viruses come with some time SMS alerts, SMS alerts when either secured or not the bank's responsibility to check.
- Change the password after 6 months.
- Remember the id and password, don't write it anywhere.
- Don't give any of the personal information to any web site that does not use encryption or other secure methods to protect it.
- Don't share any information to any one regarding to account
- Install good antivirus programmes on the system and regularly updates the programme.
- Maintain the equilibrium between usability, productivity and security.

8. CONCLUSION

With the development of the security technology and mechanism of the internet banking, as well as the gradual improvement of the security solutions of the internet banking systems, the internet banking is becoming more and more secure. We found that all banks whether public or private use latest technology for online security features but still they have some loop in this feature. The Reserve Bank of India (RBI) that is the main body, issue various directions and recommendations from time to time to strengthen cyber security of banks operating in India. Security issues include adoption of internationally accepted state-of- the art minimum technology standards for access control, encryption / decryption (minimum key length etc), firewalls, verification of digital signature, Public Key infrastructure (PKI) etc by banks.

In order for electronic banking to continue to grow, the security and the privacy aspects need to be improved. With the security and privacy issues resolved, the future of electronic banking can be very prosperous. The future of electronic banking will be a system where users are able to interact with their banks "worry-free" and banks are operated under one common standard. The biggest threat to the online security is the lack of awareness level in the users about the security challenges and banks also don't have any user awareness program to spread information. Further, most of the users do not

use online facilities because they don't have proper information and the reason behind all this is the same, which is the lack of awareness. It is also correct to say that the user also have to increase their awareness level because this is not only the responsibility of the banks but also it is for the benefit of the user. In future these technologies will increase rapidly and user will have to use these facilities so it is the requirement of the time that the user as well as the bank should make this system more secure.

REFERENCES

Books

[1] DR.B.R Sharma, BANK FRAUDS- Prevention and detection, Universal Law co.., New Delhi, Publishing Year 2009

[2] R.P Nainta, Banking System, Frauds and Legal Control, Deep & Deep Publications Pvt. Ltd. New Delhi, Publishing year 2005.

[3] D.P. Gupta & R.K Gupta, Practical Guide for prevention of FRAUDS IN BANKS, Taxmann Allied Services Pvt. Ltd. New Delhi, Publishing year june 2005.

[4] James Vadackumchery, Bankers Safety – Methods and Techniques, concept Publishing Company, New Delhi Publishing Year 2002.

[5] MACMILLAN, Security In Electronic Banking, Macmillan Publishers India Limited., Publishing Year 2007.

Websites

1) http://indiatoday.intoday.in/
2) http://cybercellmumbai.gov.in/
3) http://www.legalserviceindia.com/
4) http://eziniearticles.com/
5) http://www.rbi.org.in/
6) http://www.en.wikipedia.org/

Magazines

1) Business today {India Today Group}
2) Outlook business {Outlook Group}
3) Business India {Business India Publications Ltd.}
4) Business World {Business World Publishing Corporation}
5) Outlook Money {Outlook Group}
6) Money Today {India Today Group}
7) Forbes India {Forbes Publishing Company}
8) RBI Bulletin {RBI}

Newspaper

1) Economic Times {Bennett, Coleman & co. Ltd.}
2) Business Standard {Business Standard Ltd.} (BSL)
3) Hindustan Times Mint (HT Media Limited}
4) Financial Express {Indian Express group}
5) Financial Cronical {Financial Chronicle Publisher Pvt. Ltd.
6) Business Line {The Hindu Group Of Publication}