Volume 5, Issue 12, December 2015 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Online Banking and Cyber Attacks: The Current Scenario

Dr. Manisha M. More
Asst. Professor
Indira Institute of Management
Pune, Maharashtra, India

Meenakshi P. Jadhav
Research Scholor
Pune, Maharastra,
India

Dr. K. M. Nalawade
Principal
Kranti Agrani G.D. Bapu Lad
Mahavidyalay, Kundal, India

Abstract:** In the era of globalization Internet banking or online banking has revolutionized an integral activity of our modern twenty first century. The man developed various ways for communication to the exchange of information, ideas and knowledge which is of great importance to him as a social being. The evolution of e-banking technology makes the task very easy, banking transactions becomes very fast within a click. Online and mobile banking make daily banking fast and convenient. The misuse of information technology in the cyber space is clutching up which gave birth to cyber crimes at the national and international level. The percentage of risks and the challenges associated with it is increased. However online and mobile banking is never 100 per cent safe. The purpose of this research paper is to review current scenario of o*nline *b*anking and *cyber a*ttacks*.In this paper we focused on cyber crimes related to online banking and new tricks and techniques used by hackers. This paper also gives the details on Indian cybercrime Statistics. The latest cybercrime news related to online banking is also identified in this paper. The study totally based on the secondary data. To review and analyze the current scenario of cybercrimes, we focused on the annual reports of National Crime Record Bureau (NCRB), Indian Computer Emergency Response Team (CERT), Internet Crime Complaint Center (IC3) ,the Global Information Security Survey 2014-15, Press Information Bureau English Releases, Reserve Bank of India publications. The findings of this research paper shows that the IT usage and cybercrime related to online banking in India are on the rise. Majority of the cybercrimes have been committed by young people in the age group 18-30and are male gender. Our law enforcement agencies need to be adequately equipped to overcome and prevent the cyber crime. Finally researcher has given some suggestions for the prevention and safety use of online banking services.

***Keywords:** Information Technology, cyber crimes, cyber attacks*, mobile banking, online banking *, National Crime Record Bureau, hacking.*

I. INTRODUCTION

Information technology has played very important role in the field of banking. Online banking or e-banking is an electronic payment system that enables customers of a financial institution to conduct financial transactions on a website operated by the institution, such as a retail bank, virtual bank, credit union or building society.

Banking in India in the modern sense originated in the last decades of the 18th century. Since that time the banking sector applying different ways to provide facilities to a common man regarding to money. The banking sector is totally changed after the arrival of Internet especially in terms of security because now money is in our hand on a single click. User has number of choices to manage his money with different kind of methods.

E-banking implies provision of banking products and services through electronic delivery channels. It is method of banking in which the customer conducts transactions electronically via the Internet. It is also known as electronic funds transfer (EFT), is simply the use of electronic means to transfer funds directly from one account to another, rather than by check or cash.

The high connectivity to the world from any place has developed many crimes and these increased offences. Cyber Crimes Attack is also called Computer Network Attack is an attack from one computer to another computer using a network deliberately to alter, disrupts, deny, degrade or destroy or damage the data hosted in the attacked system or network. The interrupter interrupts by producing a malicious code which is directed against a computer processing code or logic. These attacks are made in a way to steal the relevant information without leaving back any traces of intrusion.

Financial crime, also referred as white-collar crime, covers a wide range of criminal offences which are generally international in nature. Cyber attacks generally refer to criminal activity conducted via the Internet. These crimes affect private individuals, companies, organizations and even nations, and have a negative impact on the entire economic and social system through the considerable loss of money incurred. These attacks can include stealing an organization’s intellectual property, confiscating online bank accounts, creating and distributing viruses on other computers, posting confidential business information on the Internet and disrupting a country’s critical national infrastructure. The loss or misuse of information assets is the most significant consequence of a cyber attack.

II. LITERATURE REVIEW

1. **BBC NEWS (**27 March 2015) -**Losses from online banking fraud rose by 48% in 2014 compared with 2013 as consumers increasingly conducted their financial affairs on the internet.** The rise is due to increased use of

computer malware and con-artists tricking consumers out of personal details. Overall losses on UK cards from fraud totaled £479m in 2014, up 6% on 2013, according to Financial Fraud Action. The total amount of fraud is down 21% from the peak of £609.9m in 2008. The figures also showed that losses caused by criminals using UK cards fraudulently abroad, where they can circumvent some security features, were up sharply. Losses increased to £150.3m in 2014, up 23% from the previous year. The figures come in the same week as fraud prevention service Cifas said that 46-year-old men were the most likely victims of identity theft.

2. **Business Standard** (Mumbai July 10, 2015 Last Updated at 00:41 IST) With the increase in banking on mobile phones and the internet, financial frauds in the system have also seen an uptick, says a survey on financial frauds in the financial sector by Assocham and PwC. The report said that financial frauds led to approximately $20 billion (Rs 1.26 lakh crore) in direct losses annually. The report states that currently, 74 per cent of the population has mobile phones and this has led to a steady rise in banking on the go. According to Reserve Bank of India data, the volume of mobile banking transactions has risen from around Rs 1,819 crore in 2011–12 to approximately Rs 1,01,851 crore in 2014-15. Whether it's financial transactions, customer experience, marketing of new products or channel distribution, technology has become the biggest driver of change in the financial services sector. Most financial institutions are therefore insisting on cashless and paperless transactions.
3. **Business Insider India** (Jan 5, 2015) - consulting arm of Mahindra Group, suggests that the number of cyber crimes in the country is expected to double and cross the 3-lakh mark in 2015. As per the study, the cyber crimes are growing at a rate of 107% year on year while registering over 12,000 cases every month. According to the report, the number of cases of cyber crimes was 13,301 cases in the year 2011, which was followed by 22,060 such cases in 2012 and 71,780 cases in 2013. By May 2014 alone, the cyber cells in India had registered a whopping increase in cyber crime cases and registered 62,189 cases. The increasing use of mobile, smart phones, tablets for online banking and financial transactions has also increased the vulnerabilities to a great extent. The maximum offenders came from the 18-30 age groups, stated the report. The economic growth of any nation and its security whether internal or external and competiveness depends on how well is its Misuse of the ATM-cum-debit card had been a common problem for all. Often debit card users report fraudulent transactions have been made through their ATM cards even when the cards were in their possession.
4. **Worldlypost(Karthik /January 5,2015) 1.-** Assocham-Mahindra SSG study has released a report stating the number of cyber crimes in India may double to 3 lakhs in 2015. India now being the favorite and easy to target for cybercriminals, mostly hackers, other malicious users could pose serious economic and national security challenges. India has been prone for all the identity theft, spamming, phishing and other types of fraud, as there is an upturn usage of Smart phones and tablets for online banking and other financial transactions in recent times. The Study also revealed that "the US, Europe, Brazil, Turkey, China, Pakistan, Bangladesh, Algeria and the UAE" are the countries from where most of the cyber space attacks have been originated, which is a major concern. India ranks third after Japan and US in the list of countries most affected by online banking malware during 2014. As per the study, Andhra Pradesh, Karnataka and Maharashtra are in top three positions in 2014 when it comes to the number of cyber crimes cases registered under the new IT Act in India. It further added, these three states together contribute more than 70 percent to India`s revenue from IT and IT related industries
5. **PTI New Delhi (January 5, 2015 7:04 pm):** The increasing use of smart phones and tablets for online banking and other financial transactions have increased risks. Rising at an alarming rate, the number of cyber crimes in the country may double to 3 lakh in 2015 and could pose serious economic and national security challenges. India has emerged as a favorite among cybercriminals, mostly hackers and other malicious users who use the Internet to commit crimes such as identity theft, spamming, phishing and other types of fraud. As per the study's findings, total number of cyber crimes registered during 2011, 2012, 2013 and 2014 stood at 13,301, 22,060, 71,780 and 1, 49,254 respectively. The origin of these crimes is widely based abroad in countries like China, Pakistan, Bangladesh and Algeria, among others. Phishing attacks of online banking accounts or cloning of ATM/debit cards are common occurrences. Maximum number of offenders belong to the 18-30 age group, added the report. The study revealed that the attacks have mostly originated from the cyber space of countries including the US, Europe, Brazil, Turkey, China, Pakistan, Bangladesh, Algeria and the UAE. It further stated that mobile frauds are an area of concern for companies as 35-40 per cent of financial transactions are done via mobile devices and this number is expected to grow to 55-60 per cent by 2015.Rising Internet penetration and online banking have made India a favorite among cybercriminals, who target online financial transactions using malicious software (malware). India ranks third after Japan and US in the list of countries most affected by online banking malware during 2014, the study said. Andhra Pradesh, Karnataka and Maharashtra have seen the highest number of cyber crimes registered under the new IT Act in India. Interestingly, these three states together contribute more than 70 per cent to India's revenue from IT and IT related industries

III. OBJECTIVES

To ascertain the current scenario of cyber crimes in India the following are objectives.

1. To analyze the categories of cyber crimes in banking sector.
2. To review the tricks/ techniques used by cyber criminals.
3. To review the current scenario of cyber crimes.
4. To provide set of instructions to be followed as a victim of cyber crime.
5. To suggest the preventive measures and safety tips to control and prevention of cyber crimes.

IV. METHODOLOGY USED

This study is based on secondary data. To fulfill the first objective of the study the category of cyber crimes is analyzed by reviewing various literatures and Information Technology Act 2000 as well as the web site of cyber crime investigation cell Mumbai. To review the tricks and techniques used by cyber criminals to hack the banking systems and make the cyber frauds various case studies in various news channels are referred. To review the status of cyber crimes in India and Maharashtra the data is gathered from annual reports of National Crime Record Bureau (NCRB).

1) Various Cyber attacks

Viruses and worms

Viruses and worms are computer programs that affect the storage devices of a computer or network, which then replicate information without the knowledge of the user.

Spam emails

Spam emails are unsolicited emails or junk newsgroup postings. Spam emails are sent without the consent of the receiver — potentially creating a wide range of problems if they are not filtered appropriately.

Trojan

A Trojan is a program that appears legitimate. However, once run, it moves on to locate password information or makes the system more vulnerable to future entry. Or a Trojan may simply destroy programs or data on the hard disk

Denial-of-service (DoS)

DoS occurs when criminals attempt to bring down or cripple individual websites, computers or networks, often by flooding them with messages.

Malware

Malware is a software that takes control of any individual's computer to spread a bug to other people's devices or social networking profiles. Such software can also be used to create a botnet a network of computers controlled remotely by hackers, known as herders to spread spam or viruses.

Scareware

Using fear tactics, some cyber criminals compel users to download certain software. While such software is usually presented as antivirus software, after some time these programs start attacking the user's system. The user then has to pay the criminals to remove such viruses

Phishing

Phishing attacks are designed to steal a person's login and password. For instance, the phisher can access the victims bank accounts or assume control of their social network.

Fiscal fraud

By targeting official online payment channels, cyber attackers can hamper processes such as tax collection or make fraudulent claims for benefits

State cyber attacks

Experts believe that some government agencies may also be using cyber attacks as a new means of warfare. One such attack occurred in 2010, when a computer virus called Stuxnet was used to carry out an invisible attack on Iran's secret nuclear program. The virus was aimed at disabling Iran's uranium enrichment centrifuges.

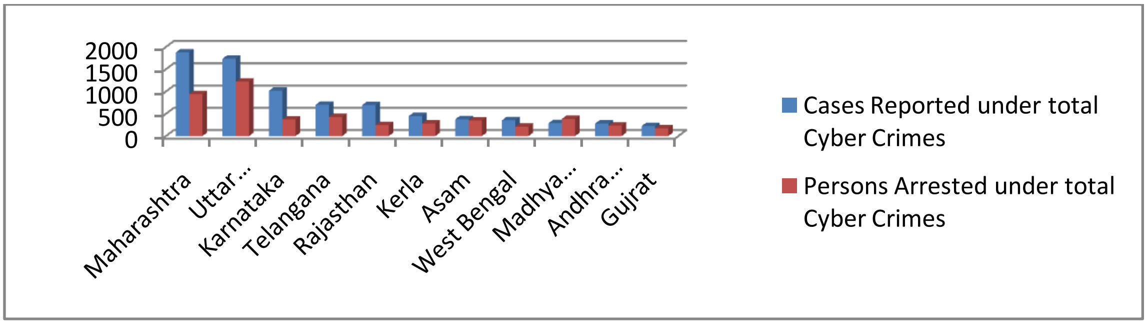
Carders

Stealing bank or credit card details is another major cyber crime. Duplicate cards are then used to withdraw cash at ATMs or in shops.

Current Scenario of Cyber Crimes Related Banking Sector in India.

Incidence of Cognizable Crimes under IT Act During 2014

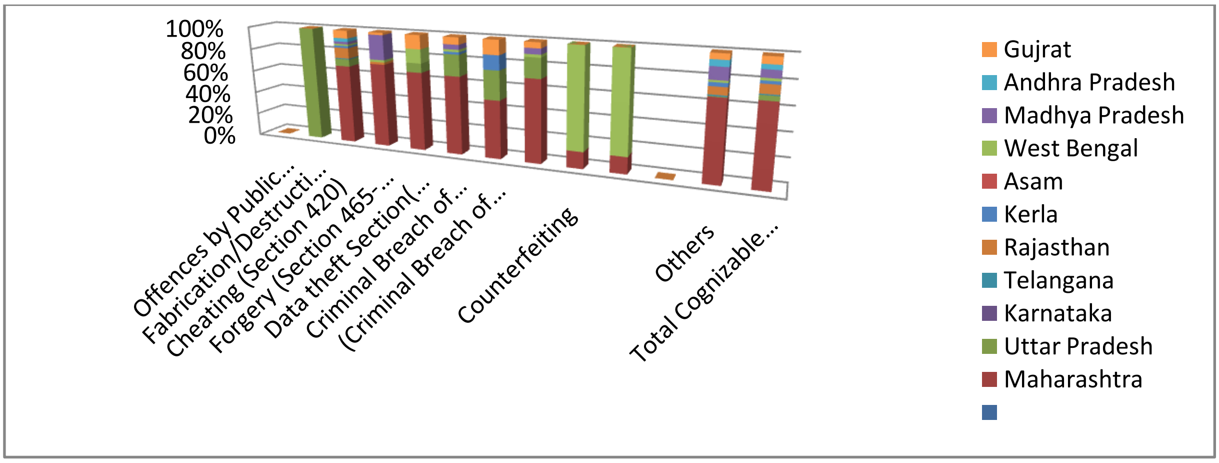
1. Cases Reported and Persons Arrested under Cyber Crime in 2014



(Source: Crimes in India 2014 Statistics)

The above graph shows the information about cyber crime cases registered and persons arrested during 2014.From the above graph it is seen that maximum cyber crimes cases are registered in Maharashtra state (1879). But compare to registration of cyber crimes cases less persons are arrested (942). Uttar Pradesh is at the second position for committing the cyber crimes (1737) and maximum persons are arrested (1223).Gujarat state is at the bottom for committing the cyber crimes.

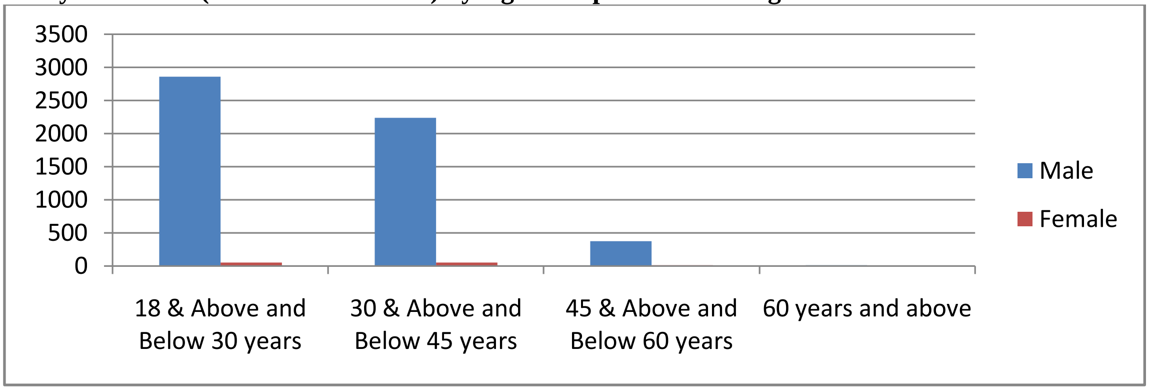
2. Incidence of Cognizable Crimes under IPC (involving Computer As Medium/Target) During 2014



(Source: Crimes in India 2014 Statistics)

Maharashtra state is at the top for committing cognizable crimes under IPC (involving Computer As Medium/Target) during 2014. Under this cheating under section 420 (671), Forgery under Section 465- 469,471& 477A (37), Data theft under section 379 to 381 (17), Criminal Breach of Trust/Fraud– debit cards & others under section 406, 408, 409 (33) are involved. Rajasthan is at second position (145). At the bottom position Karnataka state is with only 2 cognizable crimes.

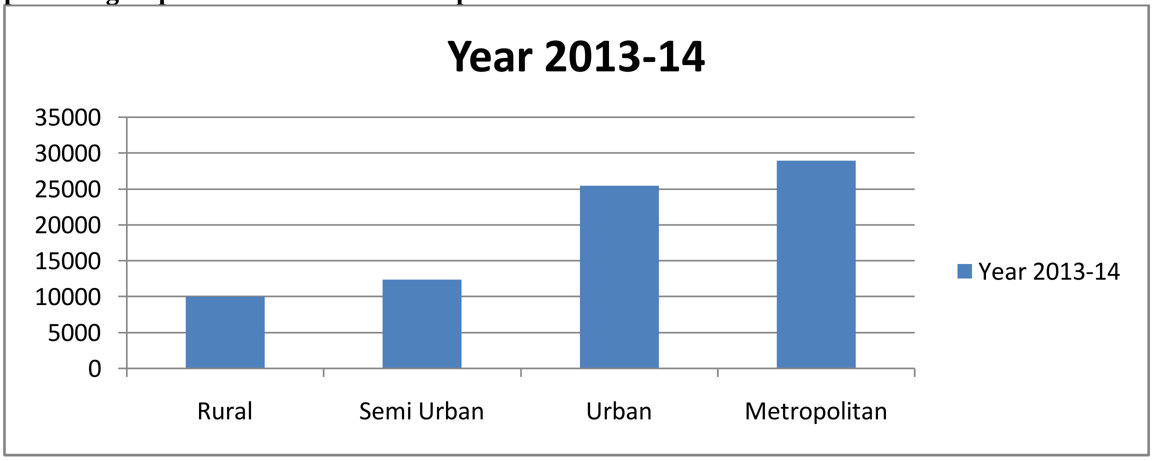
3. Total Cyber Crimes(IT Act + IPC +SLL) by Age Groups & Sex During 2014



(Source: Crimes in India 2014 Statistics)

The above graph shows the total cyber crimes under IT Act, IPC, SLL by Age Groups & Sex During 2014. It is seen that the maximum involvement of committing the cyber crimes under 18 & Above and Below 30 years age group of male (2859) is found. And only 54 females under same age groups are found. Comparative to other age groups (30 & Above, 45 & Above and 60 years and above) maximum involvement for committing the cyber crimes is found under 18 & above and below 30 age group. The involvement of the persons in 60 years & above age group is also found. As compared to the male in all age groups the female involvement for committing cyber crimes is very less.

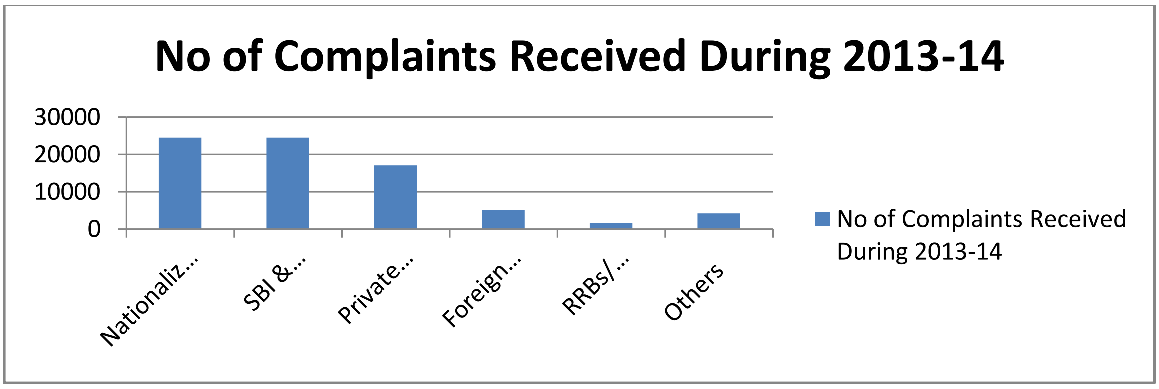
4. Population group-wise distribution of complaints received to RBI



(Source: Annual Crime Report of RBI 2013-14)

According to RBI report the distribution of complaints received from metropolitan area (28884) is more than compare to urban, semi urban and rural. Very less complaint are received to RBI from rural area (9927).

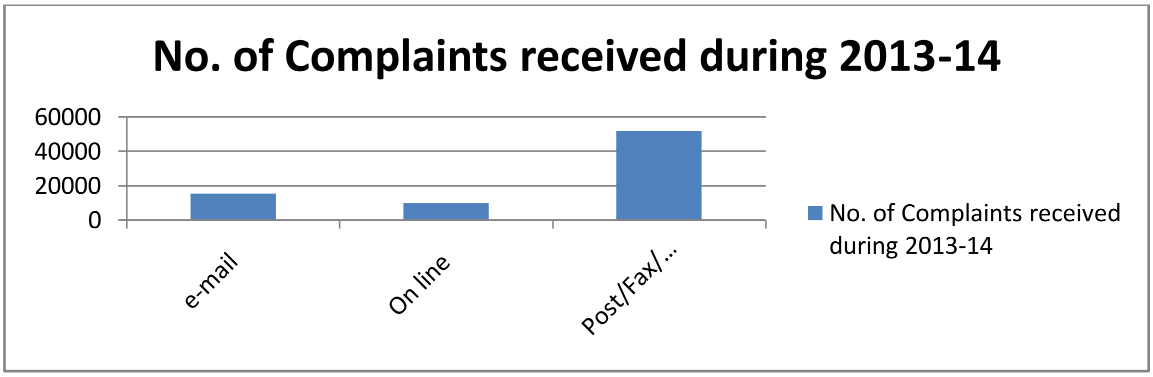
5. Bank group-wise classification



(Source: Annual Crime Report of RBI 2013-14)

The above graph shows the bank group wise classification of complaints received during 2013-14. It is seen that more complaints are received from Nationalized Banks group (24391) which follows SBI & Associates(24367), Private Sector Banks(17030), Foreign Banks(5016) and Others(4179). Very less complaint are received from RRBs/ Scheduled Primary Urban Co-op. Banks (1590).

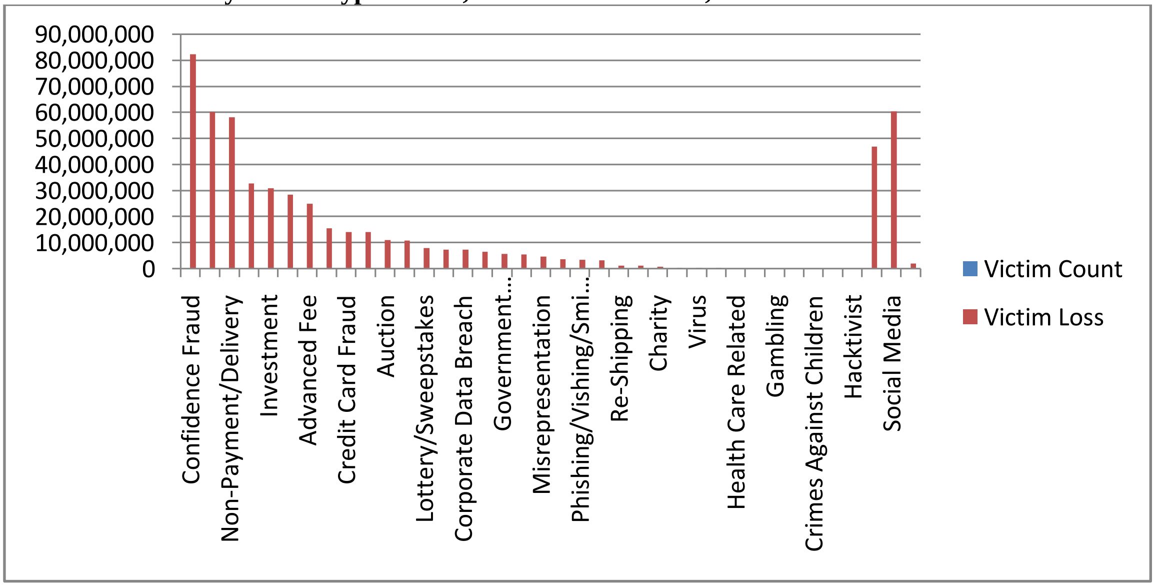
6. Receipt of complaints Mode-wise



(Source: Annual Crime Report of RBI 2013-14)

In 2013-14 Maximum complaints are received to the RBI by Post/Fax/Courier and hand delivery (51607). Very less people are using online and e-mail facility to report the complaints to the RBI.

7. Six Month Statistics by Crime Type June 1, 2014 – December 31, 2014



(Source: Six Month Statistics by RBI- June 1, 2014 – December 31, 2014)

The above graph shows six month statistics of RBI by crime type from June 1, 2014 to December 31, 2014. It shows various crimes as per the type of crime, total number of victims and total loss in dolor. It is seen that maximum victims are found under non-payment and delivery (Victims-31760 and Loss- $58139846).This graph shows various cyber crimes and victims under these cyber crimes. These are social media(Victims-9833 and Loss-$60418243) credit card fraud (Victims-7783 and Loss-$14236939), phishing(Victims-6495 and Loss-$3560332), virus(Victims-421 and Loss-$398979),Malware(Victims-819 and Loss-$314764),Denial of services(Victims-417 and Loss-$273761), Gambling(Victims-48 and Loss-$134962), Hacktivist(Victims-40 and Loss-$1058),Personal data breach(Victims-5145 and Loss-$5493229), corporate data breach(Victims-393 and Loss-$7316372), virtual currency(Victims-392 and Loss-$1972312).

2) Preventive Measures to Control Cyber Crimes in Banking Sector.

Challenges

Fighting and preventing cyber criminals from damaging infrastructure is very serious challenge to our law and enforcement agencies. It is often difficult to determine the cyber criminal and their community. The techniques used by cyber criminals are continuously evolving and making it more challenging. The following are some challenges of cyber crimes related to mobile and online banking.

1. **Tracking the origin of crime-** Tracing cyber criminals is very difficult because criminal investigations and criminal activity itself is borderless by nature.
2. **Growth of the underground cyber crime economy -**the fight against cyber crime is the growth of an underground cyber crime economy. The underground economy attracts many digital experts and talented individuals with a specialty around cyber initiative.
3. **Shortage of skilled cyber crime fighters-** skilled manpower is requiring implementing cyber security measures and encountering such cyber attacks.
4. **Widespread use of pirated software-** the most important challenge is preventing the cyber crime. The prevalence of software piracy, as pirated software is more prone to attacks by viruses, malware and Trojans.

Safety Tips for Online Secure Transaction:

1. **If the network is not properly secured**- avoid online banking, shopping, entering credit card details, etc Check your online account frequently and make sure all listed transactions are valid
2. **Never ever click on a link-** Be extremely wary of e-mails asking for confidential information they could be phishing e-mails from fraudsters. Donot click on link given in a spam e-mail.
3. **Always delete spam-**delete spam e-mails immediately and empty the trash box to prevent clicking on the same link accidentally.
4. **Beware of lotteries**- please beware of lotteries that charge a fee prior to delivery of your prize. Do not respond to lottery messages or call on the numbers provided in the text messages.
5. **Check if the website is secure**- While using a credit card for making payments online, check it if website is secure as the CVV will also be required for online transactions, is printed on the reverse of credit card. Do not provide photocopies of both sides of the credit card to anyone.It can be mis used by the fraudsters for online purchases.
6. **Notify your bank/credit card issuer** - if you do not receive the monthly credit card statement on time, if a credit card is misplaced or lost, iimmediately inform to your bank/ credit card issuer.
   Do not share bank credentials **in public** or over phone

V. CONCLUSIONS

In India the cyber crimes are rising significantly. The offences such as social media, credit card fraud, phishing, and virus, Malware, Denial of services, Gambling, Hacktivist, Personal data breach, corporate data breach and virtual currency are repeatedly done by cyber criminals. Involvement of male gender for committing cyber crimes is more in age groups 18-30 compare to female .The 60 and above age groups persons are also involved in cyber crimes. It is not good sign that senior citizens are also involved in cyber crimes. In the state wise cyber crimes list, Maharashtra is at top position. Most of the cyber crimes are committed at Nationalized Bank Group. From various categories of banks, maximum victims are suffered from money loss and data loss. The internet is the medium for huge information and medium of communication around the world, it is necessary to take certain precautions while operating it. To prevent the cyber crimes it is necessary to take certain precautions while operating the computer or internet. It is very important to educate every one and make them aware of cyber crimes and punishments –penalties for safe surfing and browsing, make them aware how to use and handle mobile and online banking, how to secure personal information, how to use various applications, what precautions has to be taken while doing online banking transactions. It is necessary to strong enforcement of cyber crimes rules and regulations.

REFERENCES

[1] Manisha M. More and Dr. K. M. Nalawade(2014) :Cyber Crimes and Attacks: The Current Scenario,1st National Conference organized by NESGOI, Pune.

[2] Susheel Chandra Bhatt and Durgesh Pant(2011): Study of Indian Banks Websites for Cyber Crime Safety Mechanism,(IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 2, No.10, Jayshree Chavan(June 2013): Internet Banking- benefits and challenges In An Emerging Economy, International Journal of Research in Business Management (IJRBM) ,Vol. 1, Issue 1, 19-26.

[3] Rupinder Pal Kaur(Aug.2013)-Statistics of Cyber Crimes in India: An Overview, International Journal of Engineering and Computer Science ,Vol 2,Issue 8.

[4] National Crime Record Bureau: Cyber Crime Statistics In India 2014: http://ncrb.gov.in/pdf

[5] Computer Emergency Response Team(CERT):http://cert.India.com

[6] Cyber Crime complaints 2015:http://rbi.org.in/Press-release

[7] Kevin Peachey (27 March 2015) Online banking fraud 'up by 48%', BBC NEWS , Personal finance reporter From the section Business retrieved from: http://www.bbc.com/news/business-32083781.

[8] BS Reporter (Mumbai July 10, 2015 Last Updated at 00:41 IST)- Cyber frauds on rise with increase in digital banking: Assocham -PwC, Business Standard, retrieved from : http://www.business-standard.com/article/finance/cyber-frauds-on-rise-with-increase-in-digital-banking-assocham-pwc-115070901104_1.html.

[9] Purba Das (Jan 5,2015,03.48 PM)- cyber crimes to surge in India Likely to Touch 3 Lakh, Business Insider, Retrieved from:http://businessinsider.in/cyber-crimes-to-surge-in-India-Likely-to-touch.

[10] Karthik (January 5,2015),Cyber crime to Double in India by 2015: A Report , world post

[11] PTI New Delhi (January 5, 2015 7:04 pm): Cyber crimes in India likely to double Published, retrieved from URL-http://indianexpress.com/article/technology/technology-others/cyber-crimes-in-india-likely-to-double-in-2015.

[12] Cyber Crime: A Financial Sector View, Government and Public Sector, NASSCOM.

[13] Assocham India: Cyber crimes in India, study by 2015, The Associated Chambers of Commerce & Industry of India

[14] History of Banking: http://en.wikipedia.org.wiki/Banking_in_India.

[15] Cyber crime News: http://timesofindia.indiatimes.com/tech/tech-news/cybercrimes-up-across-India-Maharashtra-tops.

[16] Cyber Crime News:http://ibnlive.in.com/news/cyber-crimes-up-by-51-percent-india-Maharashtra-ap-Karnataka-top-list.

[17] Cyber crime News:http://www.computerweekly.com/news/2240215532.Financial-services-sector-attract-most-cyber-crime.