IOSR Journal of Business and Management (IOSR-JBM)
e-ISSN: 2278-487X, p-ISSN: 2319-7668. Volume 19, Issue 11. Ver. IV (November. 2017), PP 60-63
www.iosrjournals.org

E-Banking & Cyber-Crime

Ms.SukhwinderKaur (Assistant Professor)
Sant Baba Bhag Singh Memo. Girls College Sukhanand (Moga)

Abstract: *The Indian banking industry has enjoyed the ride of emerging technology to undergo significant changes. Banks areamong the biggest beneficiaries of the Information Technology revolution and have largely adopted IT solutionsfor rendering the banking services to their customers.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 growing trends of cyber frauds including off line and online financial crimes are affecting a large number of people. Financial frauds with online payments, Mobile banking, ATM machines, Mobiles data, Electronic cards and net banking transactions are some challenges faced by banking concerns.This paper focuses on the different types of cybercrimes which plague the banking sector and explained about measures to aid in the combating the resulting cyber-attacks so that such attacks can be better prevented in the future for enhanced security*
Keywords*: Cyber Crime. Banking, Information Technology*

Date of Submission: 07-11-2017 Date of acceptance: 21-11-2017

I. Introduction

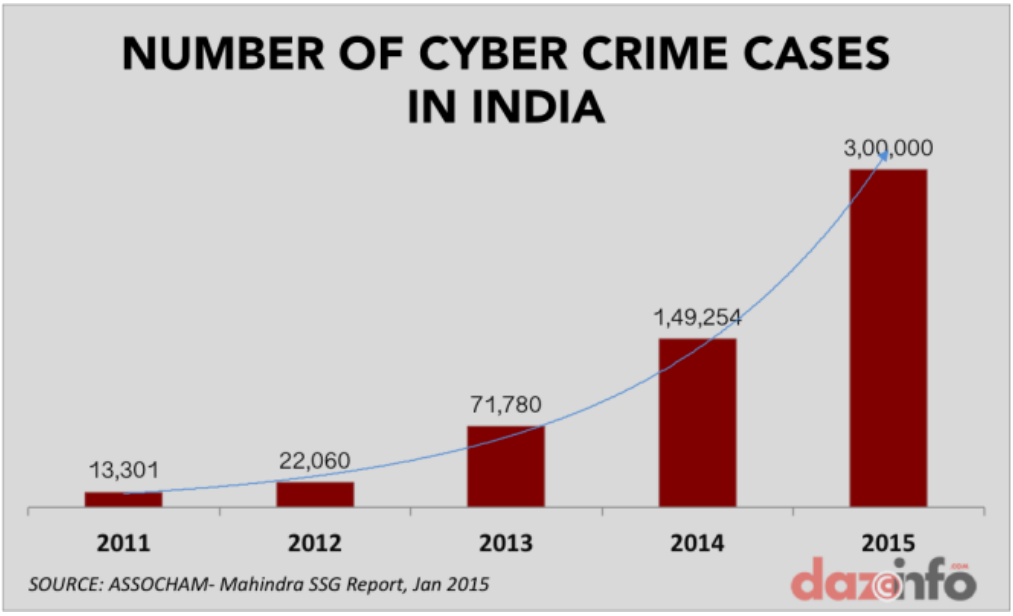
Banking in India in the modern sense originated in the last decades of the 18th century. Since that time the banking sector applying different ways to provide facilities to a common man regarding to money. The banking sector is totally changed after the arrival of Internet especially in terms of security 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 cheque or cash.With the advancement of technology and expansion of internet in banking sector, this area becomes easy to access but it also provide a pathway to commit crimes easily without any effort only sitting on a system.Cyber-crime mainly consists of unauthorized access to Data and data alteration, data destruction, theft of funds or intellectual property. Simply stated, "Cyber-Crime" is crime that involves a computer and a network.Cyber-Crime is being considered a serious threat to all the aspects of a nation's economic growth as maximuminstances of the same are being observed in financial institutions.Cyber-Crime incidents include but are not limited to credit card fraud, spamming, spoofing, e-moneylaundering, ATM fraud, phishing, vishing, identity theft and denial of service.

II. Literature Review

Cybercrime according to Douglas and Loader (2000) can be defined computer mediated activities conducted through global electronic networks which are either illegal or considered illicit by certain parties.

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.

Chakrabarty (2013) noted in his speech that, while most numbers of frauds have been attributed to private and foreign banks, public sector banks have made the highest contribution towards the amount involved.



Typesof Cyber Crime in Banking Sector:

Cyber Crimes can be broadly classified into categories such as cyber terrorism, Cyber-bullying, Software Piracy, Identity Theft, Online Thefts and Frauds, Email Spam and Phishing and manymore.However, from the aspect of financial cyber-crimes committed electronically, the following categories arepredominant:

- **Hacking:**It is a technique to gain illegal access to a computer or network in order to steal, corrupt, or illegitimately view data.
- **Phishing:** It is a technique to obtain confidential information such as usernames, passwords,and debit/credit card details, by impersonating as a trustworthy entity in an electronic communication and replay the same details for malicious reasons.
- **Vishing:** Itis the criminal practice of using social engineering over the telephone system to gain access to private personal and financial information from the public for the purpose of financial reward.
- **E-mail Spoofing**: It is a technique of hiding an e-mail's actual origin by forged the e-mail header toappear to originate from one legitimate source instead of the actual originating source.
- **Spamming**: Unwanted and unsolicited e-mails usually sent in bulk in an attempt to force the messageon people who would not otherwise choose to receive it are referred to as Spam E-mails.
- **Denial of Service:**This attack is characterized by an explicit attempt by attackers to prevent legitimate users of a service from using that service by "flooding" a network to disallow legitimate network traffic, disrupt connections between two machines to prohibit access to a service or prevent a particular individual from accessing a service.
- **Advanced Persistent Threat:**It is characterised as a set of complex, hidden and on-going computer hacking processes, often targetinga specific entity to break into a network by avoiding detection to gather sensitive information over a significant period of time. The attacker usually uses some type of social engineering, to gain access tothe targeted network through legitimate means. Successful advanced persistent threat campaigns canresult in costly data breaches.
- **ATM Skimming and Point of Sale Crimes:** It is a technique of compromising the ATM machine orPOS systems by installing a skimming device atop the machine keypad to appear as a genuine keypador a device made to be affixed to the card reader to look like a part of the machine. Additionally malware that steals credit card data directly can also be installed on these devices. Successful implementation of skimmers cause in ATM machine to collect card numbers and personal identification number (PIN) codes that are later replicated to carry out fraudulent transactions
- **Watering hole**: "Watering hole" attacks are considered an evolution of spear phishing attacks. They consist of injecting malicious code onto the public web pages of a website that that a small group of people usually visit.

In a "watering hole" attack scenario, the attackers wait for victims to visit the compromised site instead of inviting them with phishing messages. The efficiency of the method could be increased with exploitation of zero-day vulnerabilities in many large-use software programs such as Internet Explorer or Adobe Flash Player. Cyber criminals could easily compromise an improperly configured or updated website using one of the

numerous exploit kits available on the black market. Usually attackers hack the target site months before they actually use it for an attack.

The methods are very efficient. It's very difficult to locate a compromised website. "Watering hole" is a considerably surgical attack that allows hackers to hit only specific community, comparatively, classic phishing is less noisy

- **Pharming and Credit Card Redirection:**Pharming occurs when attackers are able to hijack a bank's URL so that when users try to access their bank's website, they get redirected to a fake site that looks like the real thing.
- **Malware based-attacks:**Malware based attacks are among the most dangerous cyber threats related to online banking services. The number of families of malicious code specifically designed for financial attacks is constantly increasing. Some of the most popular banking malware are Zeus, Carberp, Spyeye, Tinba and the recent KINS. But surely, the first three agents are considered to be the most by the security community. Zeus is the oldest of them. Numerous variants were detected during the last five years,and they have been often used to commit cyber fraud on a large scale. The first version of the Zeus Trojan was detected in July 2007, when it was used to steal information from the United States Department of Transportation.

  Almost every banking Trojan presents a group of shared capabilities, including backdoor and credential stealing features, and form grabbing. The majority of malware use has methods of attacking the "Man in the Browser."
- **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.
- **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.

Safety Tips for Online Banking

As the world advances in technology fraudsters are also advancing and becoming cleverer. These criminals continue to explore new ways to deceive people in the online world as they look for their next victim. To enjoy a secure experience, the following Safety Tips for Online Banking are being offered:

- ❖ Keep your password confidential: The password acts like a key to your web bankaccount. Sharing the password means that crooks can also access your online account. Inaddition, make your password as impersonal as possible. For example, do not use yourdate of birth, phone number, or your identity card number as your password. Crooks canaccess this information and decide to try it out. It is also advisable to keep changing yourpassword every four months. In addition, do not store your password in the computer**.**
- ❖ Beware of questionable Emails: Crooks may also send you emails asking for your personal information such as a password or pin. As we noted earlier, as time goes by,they get smarter and smarter. They have designed fake bank logos and use them whensending you an email; you may be easily lured to give personal information. You candetect fake emails from these crooks because their emails usually direct you toquestionable internet sites. In addition, you will notice that they do not address you asyou are used to being called by your bank. The emails may also contain poor grammar.
- ❖ Make use of anti-virus protection software: You should get the best quality antivirusprotection available for your internet banking experience. They protect yourpersonal information in your computer from being lost due to a virus. Search for theservices of a computer expert to enable you to get the top rated services available.
- ❖ If you discover you did submit private detail to these con artists, inform your webbank immediately: Make sure you give your bank your current contact information sothat they can get in touch with you with any questions or any other matters that requireyour attention.
- ❖ Ensure you have strong computer expertise to improve the safety of your personalinformation: Otherwise, avoid shared computers.
- ❖ If you notice that some money is missing in your internet bank account, notify thebank immediately: The more time that passes the more money can be stolen from you.

III. Conclusion

It's too easy to predict an increase of cyber-attacks against online banking services. However, it can be concluded the cyber security measures placed by financial institutions to curtail the curse ofcybercrime are being out- paced by dynamic technological landscape and improved expertise of the intruders With the increasingly notable impact of the peril of cybercrime, it has been continuously realised that local lawenforcement agencies do not have the required skills and resources to investigate incidents related tocybercrimes. Engagement of specialized cyber security professionals is a step further to derive quicker and better cybercrime investigation result.

Reference

[1]. Goel S (2016)Cyber-Crime: A Growing Threat To Indian Banking Sector "International Journal of Science Technology and Management" (5) (12)

[2]. Raghavan A.R., Parthiban L (2014) The Effect of Cybercrime on Bank's Finances "International Journal of Current Research and Academic Review" (2) PP: 173-178.

[3]. Kaur R.P. (2013) Statistics of Cyber Crime In India: An Overview "International Journal of Engineering And Computer Science" (2)(8) PP. 2555-2559

[4]. Anonymous (2017) Online/Safety/Tips Retrieved from https://Www.Oostburgbank.Com/Pdf On 20-06-2017

[5]. Anonymous (2017)Modern-Online-Banking-Cyber-Crime Retrieved From Http://Resources.Infosecinstitute.Com on 22-06-2017

[6]. Anonymous (2017) cyber-crime in online banking Retrieved from https://www.google.co.in/search?opera&q=types+of+cybercrime+in+banking+sectoron 30-06-2017.

Ms.SukhwinderKaur E-Banking & Cyber-Crime". IOSR Journal of Business and Management (IOSR-JBM), vol. 19, no. 11, 2017, pp. 60-63.