LAW MANTRA THINK BEYOND OTHERS
(International Monthly Journal, I.S.S.N 2321 6417)
Journal.lawmantra.co.in www.lawmantra.co.in

CYBER CRIME IN BANKING SECTOR BY MR. DIGPAL SINGH H. RATHORE & MR. KARN MARWAHA*

Introduction

A crime is an unlawful act which is not to be measured by the issue of occasions, but with the lawful aims and by the bad intentions of men. The greatest crime does not emerge from a need of feeling for others but from an over sensibility for ourselves and an over indulgence in our own desires. Cyber crime is a crime committed on the internet. This is a broad term that describes everything from electronic commerce sites to lose money

Cyber crime is a digital wrong doing. Any illegal activities committed using a computer or by using the net is known as cyber crime. Digital criminal acts are a variety of wrongdoings, which utilize machines and network systems for criminal exercises. The distinction between customary unlawful acts (Traditional crime) and digital wrong doings is the digital law violations can be transnational in nature. Cyber crime is a crime that is committed online in many areas using network and e-commerce. A computer can be the used for an offense when an unapproved access of computer system happens and on the other hand it influences e-commerce. Cyber crimes can be of different types, for example, Telecommunications Piracy, Electronic Money Laundering and Tax Evasion, Sales and Investment Fraud, Electronic Funds Transfer Fraud etc. The present contemporary period has replaced the customary fiscal instruments from a paper and metal based money to plastic cash as a Master card, credit card, debit card etc. This has brought about the expanding utilization of ATM everywhere throughout the world. The utilization of ATM is safe as well as advantageous and also convenient. As we all know that every coin has its two side same way in ATM system which is also known as plastic cash is safe and convenient but on the other side which can also be said as the evil side consist of misuse of the same. This shrewd side of the ATM System is reflected as ATM cheats or ATM frauds that is a worldwide burning issue. Cyber crime is emerging as a serious threat. Worldwide governments, police departments and intelligence units have started to react.

The Information Communication Technology (ICT) has revolutionalized different aspects of human life and has made our lives simpler. It has been applied in different industries and has made business processes simpler by sorting, summarizing, coding, and customizing the processes. However, ICT has brought unintended consequences in form of different cybercrimes. Cybercrimes have affected different sectors among which banking sector is one of them which have witnessed different forms of cybercrimes like ATM frauds, Phishing, identity theft, Denial of Service.

The human culture has experienced enormous changes every now and then with fast pace at social level from the earliest starting point and innovative level following the time of ascent

* LL.M, 2014-15, Gujarat National Law University, Attalika Avenue, Knowledge Corridor, Koba, Gandhinagar, Gujarat 382007

of innovations. This engineering word changes the human life in every way and each segment. Banking field is one of them. Managing an account in India began in the most recent many years of the eighteenth century. Since that time the banking sector is applying distinctive approaches to give facilities and securities to a common man with respect to cash saving. Security issues play extremely important role in the implementation of technologies specially in banking sector. Further on it gets to be more basic regarding the digital security which is at the center of managing an account in banking sector. After the arrival of Internet and WWW this saving money segment has been completely change extraordinarily in respect of security in light of the fact that now cash is in your grasp on a solitary click. Presently client has number of decisions to deal with his cash in different kind of methods. In this paper an endeavor has been made to advance different issues of Indian banks websites for cyber-crime safety mechanism and for the security instrument.

Cyber crime in banking sector

In today's globalise world to narrow down the world, banking sector provides many facilities to their clients and customers facilities like internet banking, credit card facilities debit card facilities online transfer by this all kind of facilities banks customer can use bank facilities 24 hours and also they can easily transect and easily operate their account from any place of the world with the help of net and mobile. As we all known that as this facilities are beneficial for the customer but it also have an evil side in which hackers and thefts are included. They make the misuse of such facilities and by hacking banking sites and customers account make a mess up in accounts and also make a robbery of the money from the customer's account for which the best example was the recent situation in which one of the hacker just take one rupee from the each account but by such one rupee he has collected lots of money. There are also many other frauds and cyber crime made in banking sectors which are mentioned below[1]

Types of cyber crime in banking sector:-

Hacking

"Hacking" is a crime, which means an unauthorized access made by a person to cracking the systems or an attempt to bypass the security mechanisms, by hacking the banking sites or accounts of the customers. The Hacking is not defined in the amended IT Act, 2000.[2] But under Section 43(a) read with section 66 of Information Technology (Amendment) Act, 2008 and Section 379 & 406 of Indian Penal Code, 1860 a person or a hacker can be punished. If such crime is proved then for such hacking offence the accuse is punished under IT Act, for imprisonment, which may extend to three years or with fine, which may be extended to five lakh rupees or both. Hacking offence is considered as a cognizable offence, it also a bailable offence.

Credit card fraud.

There are many online credit card fraud are made when a customer use their credit card or debit card for any online payment, a person who had a mala fide intention use such cards

[1] www.ijcrar.com_vol-2-2_A.R. Raghavan and Latha Parthiban
[2] Types of Cyber Crimes & Cyber Law in India, Available at http://www.csi-india.org/c/document_library/get_file?uuid=047c826d-171c-49dc-b71b-4b434c5919b6, Last visited (30/4/2015)

detail and password by hacking and make misuse of it for online purchase for which the customers card used or hacked is suffered for such kind of attract or action of a fraud made by and evil[3].

If electronic transactions are not secured the credit card numbers can be stolen by the hackers who can misuse this card by impersonating the credit card owner.

Email Fraud

In present period of life e-mail and websites are become a speedy, easy and preferred means of communication. some times by email fraud is made some of the hacker or a evil organization send email to bank customers that "congratulation you have won such a huge amount to enchase it please share your bank details" and by such customer simply have to type credit card number into www page off the vendor for online transaction or for enchase of such kind of amount then hacker make a miss use of such detail and make a crime which is also known as cyber crime as per law.

Phishing

Phishing is only one of the numerous frauds on the Internet, attempting to trick individuals into separating with their cash. Phishing alludes to the receipt of spontaneous messages by customers of financial institutions, asking for them to enter their username, secret word or other individual data to access their account for some reason. customers are directed to give a response to a mail and also directed to click on the link mentioned in the mail when they click on the given link for entering their information which were asked in the mail received by the fraudulent institution's of banking website, by such kind of activities customers thus they remain unaware that the fraud has happened with them. The fraudster then has admittance to the client's online financial balance available in the bank account and to the funds contained in that account by making the misuse of the detail received from the customer fraudulently. [4]

F-Secure Corporation's outline of 'information security' dangers amid the first 50% of 2007 has uncovered that the study discovered the banking industry as vulnerable objective for phishing tricks in India

Financial Fraud

Financial Fraud in UK, an industry body, says British misfortunes from web and phone managing account extortion climbed 59 for every penny to £35.9m in the initial six months of the year. It says that reports of fishing attacks indicate it is one of the quickest developing sorts of extortion. In response the banks have called for UK telecom groups to reduce the time people can stay on the line after someone else hangs up. By next year, most telecom operators will have cut the disconnection time to two seconds.

Accordingly the banks have called for UK telecom groups to reduce the time individuals can stay hanging before anyone else hangs up. By one year from now, most telecom administrators will have sliced the disengagement time to two seconds.

[3] Cyber law and Crimes: by Barkha Bhasin, Rama Mohan Ukkalam
[4] http://resources.infosecinstitute.com/modern-online-banking-cyber-crime/, Last visited (20/1/2015)

Fishing is one and only illustration of the continually developing digital risk that banks and their client's face, which is the reason the issue, has vaulted on to the motivation for sheets of executives, controllers and law authorization organizations.

Cyber security

Specialists say banks confront four wide sorts of risk. First, country and states use surveillance to both, take intellectual capital from banks and to destabilize them. Secondly, banks are a prime focus for cyber terrorists looking to strike against images of western capitalism. Third, purported "hacktivists" consistently make crafty endeavours to break into banks' IT organizes, normally to win more attention for their reason.[5] At long last, sorted out wrongdoing has to a great extent moved from taking cash through conventional bank heists to utilizing different means, for example, on the web, phone and card misrepresentation, which are harder to identify. [6]

Banks say controllers, for example, the Bank of England and the US Federal Reserve have been pushing them to distinguish dangers and testing their cyber strength with a project of alleged "ethical hacking". [7]

Banks are tossing tremendous assets at the issue. Before this present year's over, JPMorgan hopes to be using $250m a year on cyber security and to have prepared or contracted around 1,000 pro staff to work in the zone.

Nonetheless, cyber security specialists say banks still need to accomplish all the more, especially in pooling information and co-working on extortion and cyber risk identification. Some industry bodies do offer information on extortion and cyber assaults. On the other hand, they have limits. A few US banks are concerned that offering cyber assault information breaks security principles. UK banks just submit cases to the CIFAS business misrepresentation database when there is sufficient data to indict.

Different commercial ventures go further. British safety net providers impart all engine protection claims information to locate examples of extortion over the business and report them to the police. Banks are as of now setting up pooled utilities to impart assets on knowing your client records.

Cyber wrongdoing is apparently a significantly more imperative region where there is minimal preference to be picked up from being a pioneer in the field however an extraordinary arrangement to be lost if things happen.

Confronting a large number of assaults consistently, banks are occupied with what cyber security masters portray as "a weapons contest". They would stand a finer shot of keeping away from the destiny of JPMorgan, or more terrible, on the off chance that they pooled their assets and cooperated.

Case study

INDIA'S FIRST ATM CARD FRAUD

[5] Articles on ITA 2008
[6] Articles on IT Act 2000 & IT Rules 2011
[7] Cyber Law Cyber Crime Internet and E-Commerce by Prof. Vimlendu Tayal

The Chennai City Police have busted a global posse included in cyber crime, with the capture of Deepak Prem Manwani (22), who was discovered in the act while softening into an ATM up the city in June last, it is dependably learnt. The measurements of the city cops' accomplishment can be gagged from the way that they have netted a man who is on the needed rundown of the imposing FBI of the United States. At the time of his confinement, he had with him Rs 7.5 lakh knocked off from two Atms in T Nagar and Abiramipuram in the city. Before that, he had strolled away with Rs 50,000 from an ATM in Mumbai.

While researching Manwani's case, the police discovered a cyber crime including scores of persons over the globe. Manwani is a MBA drop-out from a Pune school and served as an advertising official in a Chennai-based firm for quite a while. Interestingly, his brassy crime vocation began in an Internet bistro. While browsing the Net one day, he got pulled in to a site which offered him support in breaking into the Atms. His contacts, sitting some place in Europe, were prepared to provide for him MasterCard quantities of a couple of American banks for $5 for every card. The site additionally offered the attractive codes of those cards, yet charged $200 for every code. The administrators of the site had conceived an entrancing thought to get the individual ID number (PIN) of the card clients. They glided another site which looked like that of presumed telecom organizations. That organization has a large number of endorsers. The fake site offered the guests to return$11.75 for every head which, the site promoters said, had been gathered in overabundance by oversight from them[8].

Accepting that it was a veritable offer from the telecom organization being referred to, a few lakh endorsers logged on to the site to get back that minimal expenditure, however simultaneously separated with their Pins. Equipped with all imperative information to hack the bank Atms, the posse started its deliberate plundering. Clearly, Manwani and numerous others of his kind entered into an arrangement with the posse behind the site and could buy any measure of information, obviously on specific terms, or just enter into an arrangement on a goods imparting premise. In the mean time, Manwani additionally figured out how to create 30 plastic cards that contained fundamental information to empower him to break into ATMS. He was enterprising to the point that he found himself able to offer away a couple of such cards to his contacts in Mumbai. The police are on the lookout for those persons as well. On receipt of vast scale grievances from the charged charge card clients and banks in the United States, the FBI began an examination concerning the undertaking furthermore alarmed the CBI in New Delhi that the worldwide posse had created a few connections in India as well. Manwani has since been developed safeguard after session by the CBI. At the same time the city police accept that this is the start of the end of a significant cyber crime.[9]

ONLINE CREDIT CARD FRAUD ON E-BAY

Bhubaneswar: Rourkela police busted a racket including an online misrepresentation worth Rs 12.5 lakh. The usual way of doing things of the charged was to hack into the eBay India site and make buys in the names of credit cardholders. Two persons, including asserted genius Debasis Pandit, a BCA understudy, were captured and sent to the court of the sub divisional judicial magistrate, Rourkela. The other captured individual is Rabi Narayan Sahu[10].

[8] http://indiaforensic.com/atmfraud.htm, Last visited (30/4/2015)
[9] http://www.indiaforensic.com/atmfraud.htm , Last visited (30/1/2015)
[10] http://www.cyberlawsindia.net/cases1.html, Last visited (30/4/2015)

Administrator of police D.s. Kutty said the pair was later remanded in legal care however four different persons purportedly included in the racket were untraceable. An argument has been enlisted against the blamed under Sections 420 and 34 for the Indian Penal Code and Section 66 of the IT Act[11] and further examination is on, he said.

While Pandit, child of a resigned representative of Rourkela Steel Plant, was captured from his Sector VII living arrangement the previous evening, Sahu, his partner and a constable, was caught at his home in Uditnagar. Pandit purportedly hacked into the eBay India site and assembled the subtle elements of around 700 credit cardholders. He then made buys by utilizing their passwords.

The extortion went to the notice of eBay authorities when it was located that few buys were produced using Rourkela while the clients were situated in urban communities, for example, Bangalore, Baroda and Jaipur and even London, said V. Naini, agent supervisor of eBay. The organization brought the matter to the notice of Rourkela police after a few clients held up grievances. Pandit utilized the location of Sahu for conveyance of the bought products, said police. The pack was included in train, flight and inn reservations.

The hand of one Satya Samal, as of late captured in Bangalore, is suspected in the crime. Samal had busy a room in a Bangalore inn for three months. The lodging and transport bills rose to Rs 5 lakh, which he didn't pay. Samal was captured for non-installment of bills, after which Pandit raced to Bangalore and stood underwriter for his discharge on safeguard, police sources said.[12]

Conclusion

Security Guardians are the most critical performing artist of this framework as they enhance the current keeping money framework and help in evacuating the vulnerabilities and advancement of frameworks so that managing an account fakes can be relieved. The security gatekeepers could be the bank itself or the some outsider enlisted by the bank to guarantee security from such dangers. If there should arise an occurrence of keeping money.

To battle these cybercrimes, the banking sector needs to team up with worldwide powers and watchdog organisations so a model can be created which can help in controlling

In conclusion I close by saying that “Thieves are not born, but made out of opportunities.” This quote precisely reflects the present environment identified with innovation, where it is changing quickly. When controller thinks of preventive measures to ensure clients from innovative frauds, either the natures turf changes itself or new engineering rises. This helps culprits to discover new regions to commit the extortion.

Cyber crime can be protected by SMS Alert facility, User Awareness Programs, Password Encryption, Virtual Keyboard, Secure Socket Layer, Short message service alerts

There is a fiendish new arrival in the world of financial fraud: Fishing. Most people have heard of phishing, which aims to trick people out of their money with an email. Fishing aims to achieve the same result, but using someone’s voice instead.

[11] Information Technology Act 2008
[12] http://www.cyberlawsindia.net/cases3.html, Last visited (20/1/2015)

What typically happens is the fraudsters give you a call, posing as a bank or credit card security team. They say there has been a problem with your account and ask you to phone the emergency number on the back of your bank card.

However, when you hang up, the fraudster stays on the line for several minutes and generates a fake dial tone. So while you think you are dialing your bank, in fact you are still connected to the conmen. They then either ask you for your account details, or – even worse – say that your account has been compromised and instruct you to move your savings to a new account they have set up.

Phishing attacks hit just about every area for example predominantly banking, e-payment systems and e-auctions. Phishing is only one of the numerous frauds on the Internet, attempting to trick individuals into separating with their cash. Now the most main problem of the banking sector which is in highest number is Phishing which is one of the cybercrime which most popular in current day. Banking sector should have to develop a strong security system to secure the customers interest and cash which is kept with the bank by the customers with a good faith that their money will be safe with the bank.

A standout amongst the most imperative approaches to moderate cyber attacks and information breaches to share data about significant incidents and cybercrime attack. Banks, law enforcement and intelligence agencies must coordinate to anticipate further harm and alleviate digital dangers that are significantly more modern.