Cybercrime: Examples and Mini-Cases

- **Official Website of Maharashtra Government Hacked,**
- **Indian Banks Lose Millions of Rupees,**
- **Parliament Attack,**
- **Pune City Police Bust Nigerian Racket,**
- **e-mail spoofing instances.**
- **The Indian Case of online Gambling,**
- **An Indian Case of Intellectual Property Crime,**
- **Financial Frauds in Cyber Domain.**

Case Study: Official Website of Maharashtra Government (Hacked Mumbai)

On 20th September 2007 IT specialists were attempting to re-control the official website of the Maharashtra government which was hacked. http:/www.maharashtragovernment.in, stayed blocked. Vice President R.R Patil confirmed that that the Maharashtra government site has been hacked. He affirmed that the state government will look into this matter and asked the Digital wrong doing Branch to examine the hacking. Patil said **if there would be need them the state would hire private IT officials for this matter**.

While, reestablishing the site disclosed to the Middle Easterner News that that programmers may have decimated majority of it's substance. IT officials said that the hackers were recognized as, **Program Cool Al- Jazeera and added that they were in Saudi Arabia.** Senior authority from government IT decision said that the official site has been influenced by infections on a few events before, however was never hacked.

Three individuals were held liable for on line Visa trick, as people were abused through online methods for booking air tickets. These parties were helped by Digital Wrongdoing Examination Cell in Pune. Mr. Parvesh Chauhan, ICICI Prudential extra security officer gripped for one of his client. As per data given by the police, one of **the client got a message for buying air tickets when the master card was held by him.** He directly went to the bank when he came to know about the issue. The tickets were booked through the online methods.

Later after examination it was disclosed that the information was gotten from State Bank of India. Shaikh was working in the Visa department and he had the information about the new clients. Further, he shared the information to Kale. Kale further passed this information to his friend Lukkad, who further booked air tickets from the acquired information and sold them for equivalent amount of money. Digital Cell head DCP Sunil Pulhari was associated for eight days and lastly caught the offenders.

Cyber Frauds In The Indian Banking Industry

The Indian Banking industry is old and many changes are brought in this industry since liberalization. The banking system is well regulated and supervised, it involves moral practice, financial distress and company governance. The call for development has given this unit monstrous probabilities and so, banks are presently among the best recipients of the IT insurgence. The on-line exchanges mounting on advancements like NEFT (National Electronic Store Exchange), RTGS (Real Time Gross Settlement), ECS (Electronic Clearing Administration) and transportable exchanges has provided aid in saving cash and fund problems.

Consequently, with the development of computers and net innovation, new forms of overall violations referred to as 'Digital Wrongdoings' has advanced within the scene. Over some years, the character and example of Digital Wrongdoing occurrences have progressively fashionable and complicated. Banks and funds connected Foundations stay the intense focuses of digital culprits within the most up-to-date decade. conspicuously financial profit is till now the important inspiration driving most cybercriminal exercises and there's token shot of this ever-changing shortly.

Indian Banks Lose Millions of Rupees

Until mid-1990s, managing an account segment in many parts of the world was basic and dependable; anyway since the coming of innovation, the keeping money division saw a change in perspective in the wonder. Banks so as to upgrade their client base presented numerous stages through which exchanges should be possible absent much exertion. These advancements empowered the client to get to their bank funds 24*7 and year around through, ATMs and Web based managing an account methods.

With the pace in innovation, the money cheating cases have increased. Cyber criminals are using different techniques to collect bank data and last their cash. Various specialized techniques have been used by the banks to safeguard these crimes, but this issue still holds on. The explanation for this is the resistance measures right now accessible with banks are accessible in the open market or area which can be used by a digital criminal, who can easily cross the safety standards. One of the techniques to relieve the issue of digital wrongdoings in keeping money segment is to distinguish the variables by banks and the issue of digital wrongdoings. Banks which are the most part focusses of digital wrongdoings experience the effects of different online assaults like phishing, keystroke logging malwares, wholesale fraud etc.

Cyber Crime in Banking Sector

Digital wrongdoing can be explained as a contravention that includes a place of wrongdoing, target, instrument, source, PC and a network as a medium. With the increased digital based business transactions, these wrongdoings have floated towards an advanced world.

These kind of digital assaults are increasing all around and India has been seeing a sharp increase in digital contravention cases in the previous few years. In 2016 an investigation by Juniper Exploration evaluated that worldwide expenses of cybercrime could be as high as 2.1 trillion by 2019.

Digital violations can be comprehensively be arranged into classification **such as digital harassing, programming robbery, wholesale fraud, Email spam, online robbery.**

The online wrongdoings can be classified as:

- Hacking: It is an unlawful access to a system to degenerate or to see any misguidedly information.
- Phishing: It includes a procedure to collect private data like username, password, one time password etc.

- Vishing: A criminal act for social designing via phone to access an individual and budgetary data from population with the goal to attain monetary benefits.
- Spamming: spontaneous messages sent to a mass population trying to constrain the message in individuals who might not get it.
- ATM Skimming and Purpose Offer Wrongdoings: It is the most developed method of trading off ATM machine or POS by introducing a gadget on the keypad which copies the same thing. Effective execution of skimmers through ATM machines gather the card numbers and personal information that are later repeated to do fake transactions

Internet Banking in India

Electronic Keeping money or e-managing an account alludes where saving money exercises are completely utilizing instructive and PC innovation over human asset. In contrast to the traditional method in e-managing there is no physical association with the banks and their customers.

E-managing is the conveyance of banks data and administration to clients by means of various conveyance stages which can be utilized through PC and mobile phones or advanced TV.[3]

A working gathering on managing was established by RBI. For the management and administration, the gatherings partitioned money into 3 categories:

1. Enlightening Framework: This category gives data about credit plans, branch areas, financing costs to the clients. The client can download different utilities according to their personal needs. There is no sensible possibility of any unapproved individual getting into the creation arrangement of the bank.
2. Open Framework: This gives data to client about his record balance. The data can be checked by clients after confirmation and signing through passwords.
3. Value Based Framework: In this category the clients can do changes through it's framework and they are directly transferred to the clients record. A bi directional change takes place between the bank and client and between client and the outsider. This framework is used trough instruments like http

and https. E keeping money incorporates Web Saving money, Portable Managing an account, RTGS, ATM's, Master Cards, Charge Cards and keen cards and so forth.

Reasons for Cyber Crime

Hart in his work, **the idea of law** has said people are helpless so standard of law is required to ensure them'. After applying this we may state that PC's are powerless so standard of law is required to secure and protect them against digital wrongdoing. Following are some reasons.

1. **Loss of proof**
2. **Negligence**
3. **Complex**
4. **Easy to access**
5. **Capacity to store information in little place.**

Impact of Cyber Crime on Banking Sector

The main cases have been identified because of the violent upsurge in cell phones with internet. Mobile phones are used for a number of online services like web saving money, paying service charges, web based shopping and is according to the criminals to acquire access to criminal data.

In the cases, where the hackers are not able to get significant data, the destroy the bank's site as a measure to render against their endeavors. Other than monetary benefits from digital assaults, the illicit business generally termed as the Darkweb[7] adds to the cybercrime as a tool for trading individual data. Touchy data including stolen Card Numbers, web based managing account, therapeutic records and authoritative access to servers are exchanged for cash in this online network

India's First ATM Card Fraud

The Chennai police busted a gang associated with digital wrongdoing. The police caught Deepak Prem Manwani aged 22 years who was caught breaking into an

ATM in the month of June. According to the police report when he was detained, he has with him Rs 7.5 lakh knocked from two ATMs in The Nagar and Abiramipuram in Chennai. Preceding that, he had left with Rs 50,000 from an ATM in Mumbai.

Manwani was an MBA dropout from a Pune school and was filled in a Chennai based firm. His wrongdoing started from a web bistro. He had some contacts who were sitting in Europe, they used to give him a card of a couple of American banks for 5 Dollars each. The administrator of the European site had an interesting plan to get individual ID Number of the clients.

That organization had a huge number of supporters. Evidently Manwani and other supporters went into the arrangement of this pack and bought a numerous information, on specific terms, are basically into an arrangement on a good sharing premise. Additionally, Manwani also learned how to create 30 plastic cards that contained important information to empower him to break ATMs.

After receiving huge number of complaints from the charged Visa clients and banks in the US, the FEI began an investigation and alarmed the CBI in New Delhi that universal pack has developed in India as well.

Findings

Maximum part of the Cybercrime consists of hacking and data fraud.

- Banks are becoming more and more focus as all the people's money is held with banks.
- The security of their clients is at huge risk since it has turned out to be anything but difficult to hack their own database.
- The quantity of cases by cyber cell has remained low throughout the previous years, with just 20 percent achieve rate.

There is no such order that deals with these violations, especially with the saving money segments.

Suggestions

1. The society should report these cases to the Digital Wrongdoing Branch rather than involving the branches for quick and strict activities.
2. Projects should be started to aware the public about the continuous situations and forthcoming situations.

3. Punishments should be practiced completely to stop these issues and punish the assailants.
4. The legislature should keep a track on the working system of Huge information banks.
5. There should be quick dispose of cases, to meet the complaints and fabricate certainty among the general public.
6. The law implementation should be strict and occasionally monitor such wrongdoings.

How to Report

With the increase in the digital world, especially when it comes to banking transactions, the risk of financial frauds cannot be ignored. A fraudulent online transaction in one's bank account, debit or credit card could be because of e-mail spoofing, phishing or it could have been an act committed by cloning one's card.

If you a fraud related to net banking or ATM transactions, or any other online transaction happens, you have to raise a complaint. But, before filing a written complaint with the bank or the card issuer, the victim must have following documents.

- Bank statement of the last six months of the concerned bank.
- Make a copy of SMSs received related to the alleged transactions.
- Take copy of your ID proof and address proof as shown in the bank records.
- Lodge a complaint in your nearest police station explaining the complete incidence along with the abovedocuments.

There are several fake apps being floating around in the cyber world. In case of any financial fraud committed through an app, in addition to the above mentioned documents, also furnish the screenshot of the malicious app and the location from where it was downloaded.

Where to File Complaint

The complaint can be filed in the nearest police station. if any of the police officer does not lodge an FIR then a direct complaint can be made to the magistrate.

Liability

Now, if the fraud happens and the bank is not at fault and it was committed by a third-party through an act of scamming, phishing etc, the RBI rules says that the customer is not required to pay if the breach has been reported within three days of the fraudulent transaction. A transaction reported after that but within seven days, the per transaction liability of the customer will be limited to the transaction value or an amount set by the central bank, whichever is lower.

Recommendations

Managing of accounts is one of the important function of our economy. The increasing number of cyber wrongdoings has brought a great lose to our economy. Cyber assaults ought to be averted by appropriate enactment which is actualised adequately. Both the clients and the banks should take appropriate shield measures. **The Indian Government has set up an Entomb Departmental Data Security Team (ISTF) with the National Security Board as the nodal organization** for the coordination of all issues identifying with viable usage of it's digital security technique.

Cyber Fraud Council in Banks

At whatever point a digital extortion is carried out the unfortunate casualty should answer to the Digital Misrepresentation Gathering that must be set up by in every single bank to audit, screen research and report about digital wrongdoing. In the event that, such Committee does not take perform or declines to play out its obligation then an arrangement to record a FIR must be made.

The issue to be brought before such gathering can be of any esteem. In any case, when the esteem is high then the Committee will act quickly. RBI in its 2011 Report expressed that when bank fakes are of short of what one Crore then it may not be important to require the consideration of the Extraordinary Advisory Group Board.

Education to Clients

The client must be aware about different bank cheats and measures should be taken to educate them for security components with the objective that they don’t fall prey as casualties of cybercrime. If a client is cognizant and reports a particular matter of cybercrime timely, then the rate of cybercrimes can be diminished. A client should be made aware of the rules and regulation of E-Managing an account. This awareness can be brought to the customers by publishing on banks site, distributing in paper, sending messages, training and so on.

On the off chance and a bank present any new strategy or there are some other progressions which are which are required to be trailed by all banks according to

RBI at that point bank must educate the client through phone.[9] The mindfulness material ought to be opportune refreshed remembering the adjustments in the enactment and rules of Reserve Bank of India.[10]

Training of Bank Employees
Introduction programs must be directed for the staff by banks. The staff must be made mindful about misrepresentation counteractive action measures. It can be done in a better way by distribution of pamphlets, through magazines. Center saving money arrangement programming having discussion on elements causing cybercrime and activities required to prevent them.

Cooperation at International Level to Curb Cybercrime
The internet is transnational in nature and requires mutual understanding between states to cooperate to turn away cybercrime. In spite of the fact that, a couple of bargains and usage estimates exist a healthy methodology characterizing legitimate and specialized measures and authoritative abilities is yet to take focal significance for India in its objective to add to the worldwide battle against cybercrime.

IT Act, 2000 having additional regional application represents an issue in examination, arraignment and removal of outside nationals. India ought to effectively connect as a feature of the worldwide cybercrime network focused on Asia, Europe and America to look for help and furthermore add to universal cybercrime issues.

Conclusion
In my opinion no sort of crime should be tolerated. The safety and privacy of an individual should be safeguarded. Every person has a right to live in a secure environment, no matter in real life or on internet.
After doing the research on this issue, I understand the motive of the cyber-criminals. To a certain extent, I see why some choose to take their political/religious protests online.

- Protestors are likely to get caught
- Online protests get due attention
- Support is gained quickly.
- Global reach through internet.

However, I find Cyber Crime more serious offence than the real life crimes, as it effects millions of web users at once. In real life it harms only a few number of persons.

When online business activities get disrupted, it leads to great problems for customers and companies. With technology being such a big part of our lifestyle today, cybercrime has no place in it. For instance, following cybercrime on Sony, the Federal Bureau of Investigation has issued search warrants to arrest the culprits. To me, it is a massive piece of news, because it indicates strengthening commitment against these criminals.

Parliament Attack Cyber Crime Case Study

Bureau of Police Research and Development at Hyderabad had handled some of the top cyber cases, including analysing and retrieving information from the laptop recovered from terrorist, who attacked Parliament. The laptop which was seized from the two terrorists, who were gunned down when Parliament was under siege on December 13 2001, was sent to **Computer Forensics Division of BPRD after computer experts at Delhi failed to trace much out of its contents**.

The laptop contained several evidences that confirmed of the two terrorists' motives, namely the sticker of the Ministry of Home that they had made on the laptop and pasted on their ambassador car to gain entry into Parliament House and the the fake IDcard that one of the two terrorists was carrying with a Government of India emblem and seal.

The **emblems (of the three lions) were carefully scanned** and the seal was also craftily made along with residential address of Jammu and Kashmir. But careful detection proved that it was all forged and made on the laptop.

A. Four foreign nationals have been arrested by Pune Police

Four foreign nationals have been arrested from Pune for allegedly cheating several people of lakhs with the promise of jobs abroad, police said on Thursday.

A team of the Cyber police from the Mumbai crime branch raided a flat in Undri area of Pune and arrested the four accused on Wednesday, an official said.

The arrested accused include Nigerian and West African nationals who allegedly got in touch with at least 2,000 job seekers of various countries and cheated them, the official said.

As many as 14 mobile phones, four laptops, three memory cards, five routers, a data card, two international SIM cards were recovered from the premises, he said.

During the investigation, the police found that the accused had transferred at least ₹ 10 crore to a Nigerian bank, he said.

The accused had collected this amount from job seekers in the form of visa fees, programme fees, employment authorisation and travel allowance, the official said.

The racket came to light on January 15, when Chembur resident Vishal Mandavkar approached the Cyber police with the complaint of online fraud, he said.

According to the police, Vishal Mandavkar had responded to an advertisement about a job at a prominent hotel in Canada and mailed his resume, following which he was asked to deposit ₹ 17.22 lakh as visa fee, programme fee, employment authorisation and travel allowance.

Once the amount was paid, the contact person stopped responding to the complainant's calls, it was stated.

B. Pune: Two Nigerians Arrested For Cloning ATM Card And Withdrawing Money

Pune, 30 April 2021: The officials from the cyber police station of the Pune city police have nabbed two Nigerian nationals for installing scammers and cameras at ATM centres and obtaining citizens’ confidential information, making fake ATM cards from it, and withdrawing money from their bank accounts.

According to the police, they received a complaint on April 28 from a person that a total of Rs 1.1 lakh was withdrawn from his account for three consecutive days without using his ATM card. The transactions took place at an ATM centre of Dharmaveer Sambhaji Urban Bank at Kasarwadi, Nashik Fata, Pune. The transactions had taken place between 6 am to 8 am.

Accordingly, the officials from the cyber police station set up a trap at around 5.30 am on Thursday (April 29) at the said ATM and nabbed a Nigerian national who was withdrawing money using the cloned cards, including that of the complainant.

The arrested foreigner has been identified as Nnam Gabriel Chukwuebuka, a resident of Pimple Nilakh. Police seized four ATM cards from his possession. During the investigation, the arrested accused told cops about another Nigerian national named Bashir alias Lucas William alias Omoike Godson who had given him the ATM cards. Police arrested Bashir from a hotel near Jagtap Dairy in Rahatani and seized 10 ATM cards from different banks, a black ATM card reader, a software CD and some red-and-white stickers from his room.

Based on a complaint from Pandurang Subhash Kanda, the cyber police station has registered an FIR against the two arrested accused of offences under Sections 419, 420, 465, 467, 471, and 34 of the Indian Penal Code (IPC) and Section 66 (c), 66 (d) of the Information Technology Act.

The action was taken under the guidance of Commissioner of Police Amitabh Gupta, Joint Commissioner of Police Ravindra Shiswe, Additional Commissioner of Police (Crime) Ashok Morale, Deputy Commissioner of Police (Economic and Cybercrime) Bhagyashree Navatake, and ACP Milind Patil.

The investigation team included Senior Police Inspector DS Hake, Police Inspectors Kumar Ghadge, Pandit and Chintaman, API Gawte, PSI Anil Daffal, and police personnel Nitesh Shelar, Sachin Waje, Anil Pundalik, Somnath Bhorde, Sandeep Yadav, Pravin Singh Rajput, Saurabh Ghate, Rahul Handal, Girimallesh Chalwadi, and Kiran Jamdade.

The Indian Case of online Gambling

The online gambling culture in India is one of the most active in the entire world. And this applies to varied aspects of betting as well. Betting on sports and casino games is deeply embedded into the identity and culture of the Indian people. The relationship that Indians have with gambling and casinos has been well-documented over the decades through spikes in the global industry. However, when it comes to the gambling laws in India, not everything is always going to be cut and dry. In fact, due to the ambiguity and vagueness surrounding gambling legislation in India, many people might actually question the legality of betting on games like online slots, poker, and baccarat.

Performing a quick search query in India will offer citizens a variety of different betting platforms that are offering all sorts of different bonuses and promotions that are looking to lure new users onto their sites. However, it still begs to ask the question as to whether online gambling in India really is legal or not. After all, more and more people are becoming more attuned to using technology in their everyday lives. These days, practically everyone interacts with a mobile smart device like a smartphone or a tablet. Aside from that, a lot of people in India now have access to high-speed internet. All of these ingredients combined have allowed for the online gambling market to flourish. But there remains to be a lot of grey area when it comes to the laws and regulations behind gambling in India.

According to the Public Gambling Act of 1867, practically all forms of gambling are illegal in India. Technically speaking, based on this act alone, placing bets on horseraces or cricket matches is prohibited. However, there are certain provisions within the law that mark a difference between games of skill and games of chance. Technically, betters are allowed to place bets on games of skill. This places a lot of ambiguity around the legislation because it's not entirely clear what constitutes the difference between a game of chance and a game of skill. This is why the betting culture is still rampant despite its technical illegality. The ambiguity allows for many establishments to circumvent certain provisions in the Public Gambling Act.

India is also divided up into various independent states that are all mandated to impose their own laws and regulations. Currently, the state of Sikkim is known to offer a more liberal stance towards online betting. In 2009, Sikkim welcomed its first casino and it now has a few lottery services that are run and operated by the state itself. The state of Goa is popular for having a wide range of luxury cruises and floating casinos that appeal to a large bulk of the tourism market. Other states around the country are more strict when it comes to the establishment of gambling operations.

Again, given the ambiguity of the law, it's still possible for most Indian residents to actually participate in online gambling. Technically speaking, casino operators are not allowed to establish their operations within the country. However, that doesn't mean that residents of India can't access offshore casino platforms. In most of India, residents have access to gambling platforms from all over the world that offer a variety of different casino games. Also, these casinos typically have their transaction mechanisms set up through third-party service providers like PayPal which are recognized worldwide. This is essentially how so many people in India are still able to participate in online gambling activities despite its technical illegality within the Public Gambling Act. To this day, no private citizen in India has ever been charged for gambling illegally.

At the end of the day, there's so much pressure on the Indian government to draft newer and more relevant pieces of legislation when it comes to gambling. This is because the potential revenues from taxes that could have been generated from regulated gambling could have helped the national economy. Aside from that, many foreign investors are eager to establish operations in India to penetrate a market that's rife with growth and potential. Ultimately, it still remains to be seen as to whether the Indian government will look to respond to these calls for more modern laws.

In fact, due to the ambiguity and vagueness surrounding gambling legislation in India, many people might actually question the legality of betting on games like online slots, poker, and baccarat. ... According to the Public Gambling Act of 1867, **practically all forms of gambling are illegal in India**