TASK 2

Case Studies on Social Media Crimes

By Kowshik Kumar Aitha

GCPCSSI 2021 INTERN

Case Studies –

Pune Citibank Mphasis Call Center Fraud

Some ex-employees of BPO arm of MPhasiS Ltd MsourcE defrauded US Customers of Citibank to the tune of Rs 1.5 crores. It was one of those **cyber-crime cases** that raised concerns of many kinds including the role of "Data Protection".

The crime was obviously committed using "Unauthorized Access" to the "Electronic Account Space" of the customers. It is therefore firmly within the domain of "Cyber Crimes". ITA-2000 is versatile enough to accommodate the aspects of crime not covered by ITA-2000 but covered by other statutes since any IPC offence committed with the use of "Electronic Documents" can be considered as a crime with the use of a "Written Documents". "Cheating", "Conspiracy", "Breach of Trust", etc. are therefore applicable in the above case in addition to the section in ITA-2000.

Under ITA-2000 the offence is recognized both under Section 66 and Section 43. Accordingly, the persons involved are liable for imprisonment and fine as well as a liability to pay damages to the victims to the maximum extent of Rs 1 crore per victim for which the "Adjudication Process" can be invoked.

SONY.SAMBANDH.COM CASE

India saw its first cybercrime conviction in 2013. It all began after a complaint was filed by Sony India Private Ltd, which runs a website called www.sony-sambandh.com, targeting Non-Resident Indians. The website enables NRIs to send Sony products to their friends and relatives in India after they pay for it online.

The company undertakes to deliver the products to the concerned recipients. In May 2002, according to the cybercrime case study, someone logged onto the website under the identity of Barbara Campa and ordered a Sony Colour Television set and a cordless headphone. She gave her credit card number for payment and requested the products to be delivered to Arif Azim in Noida. The payment was duly cleared by the credit card agency, and the transaction was processed. After following the relevant procedures of due diligence and checking, the company delivered the items to Arif Azim.

At the time of delivery, the company took digital photographs showing the delivery being accepted by Arif Azim. The transaction closed at that, but after one and a half months the credit card agency informed the company that this was an unauthorized transaction as the real owner had denied having made the purchase.

The company lodged a complaint about online cheating at the Central Bureau of Investigation which registered a case under Section 418, 419 and 420 of the Indian Penal Code. The matter was investigated, and Arif Azim was arrested. Investigations revealed that Arif Azim while working at a call Centre in Noida gained access to the credit card number of an American national which he misused on the company's site.

The CBI recovered the colour television and the cordless headphone, in this one-of-a-kind cyber fraud case. In this matter, the CBI had evidence to prove their case, and so the accused admitted his guilt. The court convicted Arif Azim under Section 418, 419 and 420 of the Indian Penal Code - this being the first time that cybercrime has been convicted.
The court, however, felt that as the accused was a young boy of 24 years and a first-time convict, a lenient view needed to be taken. The court, therefore, released the accused on probation for one year.

The judgment is of immense significance for the entire nation. Besides being the first conviction in a cybercrime matter, it has shown that the Indian Penal Code can be effectively applied to certain categories of cyber-crimes which are not covered under the Information Technology Act 2000. Secondly, a judgment of this sort sends out a clear message to all that the law cannot be taken for a ride.

The Bank NSP Case

One of the leading cybercrime cases is the Bank NSP case is the one where a management trainee of the bank was engaged to be married. The couple exchanged many emails using the company computers. After some time, the two broke up and the girl created fraudulent email ids such as "indianbarassociations" and sent emails to the boy's foreign clients. She used the bank’s computer to do this. The boy's company lost a large number of clients and took the bank to court. The bank was held liable for the emails sent using the bank's system.

BAZEE.COM CASE

CEO of Bazee.com was arrested in December 2004 because a CD with objectionable material was being sold on the website. The CD was also being sold in the markets in Delhi.
The Mumbai Police and the Delhi Police got into action. The CEO was later released on bail. This opened up the question as to what kind of distinction we draw between Internet Service Provider and Content Provider. The burden rests on the accused that he was the Service Provider and not the Content Provider. It also raises a lot of issues regarding how the police should handle cybercrime cases.

Cyber Attack on Cosmos Bank

In August 2018, the Pune branch of Cosmos bank was drained of Rs 94 crores, in an extremely bold cyber-attack. By hacking into the main server, the thieves were able to transfer the money to a bank in Hong Kong. Along with this, the hackers made their way into the ATM server, to gain details of various VISA and Rupay debit cards.

The switching system i.e., the link between the centralized system and the payment gateway was attacked, meaning neither the bank nor the account holders caught wind of the money being transferred.

According to the cybercrime case study internationally, a total of 14,000 transactions were carried out, spanning across 28 countries using 450 cards. Nationally, 2,800 transactions using 400 cards were carried out. This was one of its kinds, and in fact, the first malware attack that stopped all communication between the bank and the payment gateway.

BSNL, Unauthorized Access

In a leading cybercrime case, the Joint Academic Network (JANET) was hacked by the accused, after which he denied access to the authorized users by changing passwords along with deleting and adding files. Making it look like he was authorized personnel, he made changes in the BSNL computer database in their internet users' accounts.
When the CBI carried out investigations after registering a cybercrime case against the accused, they found that the broadband Internet was being used without any authorization. The accused used to hack into the server from various cities like Chennai and Bangalore, amongst others. This investigation was carried after the Press Information Bureau, Chennai, filed a complaint.
In the verdict by the Additional Chief Metropolitan Magistrate, Egmore, Chennai, the accused from Bangalore would be sent to prison for a year and will have to pay a fine of Rs 5,000 under Section 420 IPC and Section 66 of the IT Act.

Bomb Hoax Mail

In an email hoax, sent by a 15-year-old boy from Bangalore, the Cyber Crime Investigation Cell (CCIC) arrested him in 2009. The boy was accused of sending an email to a private news company saying, "I have planted 5 bombs in Mumbai, you have two hours to find them". The concerned authorities were contacted immediately, in relation to the cyber case in India, who traced the IP address (Internet Protocol) to Bangalore.

A Look-alike Website

A 9-person crime, was registered under Sections 65, 66, 66A, C and D of the Information Technology Act, along with Sections 419 and 420 of the Indian Penal Code.

Under the complaint of this cyber fraud case in India, a company representative in the business of trading and distribution of petrochemicals in India and abroad had filed the report against the 9 accused of using a similar looking website to carry on the trade.

The accused ran a defamation campaign against the company, causing them crores of rupees of loss from their customers, suppliers and even producers.

Cyber Terrorism

Since the changes were carried out in the Information Technology Act in Mumbai, this case of cyber terrorism was its first project. A threat email had been delivered to the BSE and NSE, at 10:44 am on Monday. With the MRA Marg police and the Cyber Crime Investigation Cell (CCIC) working together on the cyber-crime case, the accused has been detained. The IP address had been traced to Patna, Bihar. When checked for any personal details, two contact numbers were found, which belonged to a photo frame maker in Patna.

Mumbai: 15-year-old boy detained for flashing during online classes

The Police said the minor had repeatedly flashed himself in front of the teacher while she was taking online classes for Std IX between February 15 to March 2 2021

Mumbai Police have detained a 15-year-old boy for allegedly flashing his private parts at a teacher during online tutorials. The police said the minor had logged in using a fake number and email address. The police said the minor had repeatedly flashed himself in front of the teacher while she was taking online classes for Std IX between February 15 and March 2.

A police officer said, “The teacher could not see his face and the minor would repeatedly log in and commit the same crime again and again. In order to stop this, the teacher then approached the police and lodged a complaint.”

With the help of the minor’s IP address, police traced him in Jaisalmer and detained him. “When we asked him, why did you flash your private parts during online classes, the minor told us he did it for fun,” said an investigator.

Woman duped of Rs 43 Lakh by ‘Facebook friend’

Police are investigating the cell phone number from which the complainant got calls, the e-mail address used by the accused and also bank accounts in which she made online payments.

A 51-year-old woman was duped of Rs 43.3 lakh by an online fraudster who befriended her on Facebook. The victim has lodged the first information report in this case at the Cyber police station. Police said the woman, a resident of Katraj, came in contact with the accused on FB in January this year. After developing a friendship with her, the accused, who claimed to be living abroad, told her that he has sent her some costly gifts like a wrist watch, gold chain and an I-phone, in a parcel.

Then another person, who called herself Jenny, called up the complainant and asked her to pay charges towards Customs clearance, transport, Customs duty, GST and other purposes for claiming the “gifts”. As per the instructions of the accused, the complainant made online payments to the tune of Rs 43,35,000 into multiple bank accounts till May this year. But she never received her “parcel”.

Realizing that she has been cheated, she approached Pune City Police and filed a complaint against the accused. Police have booked the accused in this case under sections 419, 420, 34 of the Indian Penal Code (IPC), pertaining to cheating, and sections of the Information Technology Act. Police are investigating the cell phone number from which the complainant got calls, the e-mail address used by the accused and also bank accounts in which she made online payments.

Submitted by

Kowshik Kumar Aitha

GCPCSSI 2021 INTERN