CHAPTER – V

CYBER CRIME SCENARIO IN TAMIL NADU

This chapter puts with cyber crime scenarios in Tamil Nadu. Increase in cyber crime rate has been documented in the news media. Both the increase in the incidence of criminal activity and the possible emergence of new varieties of criminal activity pose challenges for legal systems, as well as for law enforcement.¹

There is no denying the fact that cyber crime is on rise and India cannot remain immune to this. An interesting story came to light recently in Chennai when a girl lodged a complaint with the cyber crime cell, after she was bombarded with calls on her mobile phone from strangers asking for sexual favours. Apparently, this girl’s photograph and phone number was put up on a networking site describing her as service girl.²

In order to prevent cyber crimes, the cyber crime cells were created in Tamil Nadu and infrastructures were provided.

The cyber crime cell got into action and in no time, picked up a manager of a private firm who admitted his crime. The victim and offender were one time friends but had fallen apart. The cyber crime cell issued a stern warning to such offenders that if they believe they can remain anonymous in cyberspace, they are wrong, their crime can easily get detected and they can be caught in no time.

¹ Criminal Investigation Department Review, January 2008 – Article on “Cyber Crime Scenario in India” submitted by Dr.B.Muthukumaran, Chief Consultant, Gemini Communication Limited, p.17.
² http://poundpuplegacy.org
The cyber crime cell said that instances of misuse of photographs of women are on the rise on the internet and it receives at least two such complaints every month. Sometimes photographs are morphed and used with obscene content, at times even genuine photographs are morphed and used with obscene content, at time even genuine photographs are used for that. The cyber crime cell has advised the public, especially girls against sharing of photographs, even among best friends.³

Regular stories featured in the media on computer crime include topics covering hacking to viruses, web-jackers, to internet paedophiles, sometimes accurately portraying events, sometimes misconceiving the role of technology in such activities.

**Statistical Reports on Cyber Crimes in Tamil Nadu on the data furnished by State Crime Record Bureau, Tamil Nadu Police**

In the year 2000, totally 6 cyber crimes were reported in Tamil Nadu. In which, 2 cases were related to IT Act, 2000 registered under Software Piracy and 4 cases were related to IPC sections registered under Forgery.⁴

In 2001 also, totally 6 cyber crimes were reported. In which, 3 cases were related to IT Act, 2000 and 3 cases were related to IPC sections. Of the total 3 cases registered under IT Act, 2000, 2 were related to cyber pornography and one was related to obscene publication/cyber pornography. Of the total 6 cases registered for cyber crimes under IPC, 2 cases were related to Misappropriation of funds and one was related to Fictitious trading account.⁵

⁴ *Annual Datas on Cyber Crime* furnished by State Crime Record Bureau, Tamil Nadu Police, for the year 2000.
In 2002, totally 5 cyber crimes were reported. In which, 3 cases were related to IT Act, 2000 under Threatening E-mail and 2 cases were related to IPC sections under Creating false information through computer.\(^6\)

In 2003, totally 6 cyber crimes were reported and all were under IT Act. In which, 3 cases were related to Cyber pornography, Tampering (2) and Fraud Digital Signature Certificate (1).\(^7\)

In 2004, totally 13 cyber crimes were reported and all were under IT Act. In which, 7 cases were related to Cyber pornography, Loss/Damage to computer (5) and Fraud Digital Signature Certificate (1).\(^8\)

In 2005, totally 22 cyber crimes were reported and all were under IT Act. In which, 15 cases were related to Loss/Damage to computer, Cyber pornography (5), and Tampering (2).\(^9\)

In 2006, totally 8 cyber crimes were reported and all were under IT Act. In which, 7 cases were related to Loss/Damage to computer and one was related to Cyber pornography.\(^10\)

In 2007, totally 15 cyber crimes were reported. In which, 10 cases were related to IT Act, 2000 and 5 cases were related to IPC sections under Criminal breach of trust. Of the total 3 cases registered under IT Act, 2000, 7 were related to cyber pornography, Loss/Damage to computer (2) and one was related to Tampering.\(^11\)

In 2008, totally 25 cyber crimes were reported. In which, 21 cases were related to IT Act, 2000 and 4 cases were related to IPC sections under Forgery. Of

---

\(^6\) *annual datas on cyber crime* furnished by State Crime Record Bureau, Tamil Nadu Police *for the year 2002.*

\(^7\) *Ibid., for the year 2003.*

\(^8\) *Ibid., for the year 2004.*

\(^9\) *Ibid., for the year 2005.*

\(^10\) *Ibid., for the year 2006.*

\(^11\) *Ibid., for the year 2007.*
the total 21 cases registered under IT Act, 2000, 10 were related to Loss/Damage to computer, Tampering (5), Cyber pornography (4), Unauthorised access (1) and Breach of confidentiality (1).\textsuperscript{12}

In 2009, totally 37 cyber crimes were reported. In which, 18 cases were related to IT Act, 2000 and 19 cases were related to IPC sections. Of the total 18 cases registered under IT Act, 2000, 8 were related to Hacking, Loss/Damage to computer (4), Tampering (3) and Cyber pornography (3).\textsuperscript{13}

**Special Units in Tamil Nadu Police to handle Cyber Crimes**

In Tamil Nadu, in 2002, two Cyber Crime Cells were created; one is exclusively for Chennai Police and another at CB-CID, having jurisdiction throughout State of Tamil Nadu.\textsuperscript{14} The Cyber Crime Cell was created in the Chennai City Police on 14\textsuperscript{th} November 2002. The State level Cyber Crime Cell, CB-CID was formed with the sanctioned strength of one DSP, two Inspectors, two SIs and nine other ranks including three drivers and started functioning since 5\textsuperscript{th} May 2003.\textsuperscript{15} The Unit was declared as a Police Station and the Officer in the rank DSP was declared as an officer in charge of the Police Station.\textsuperscript{16} The Cyber Crime Cell in Coimbatore was formed in August 2008. The role of these Cells is to detect, prevent and investigate Cyber crimes that come under the ambit of Information Technology Act 2000 and assist the other Law Enforcement in the investigation of crimes in which elements of Computer related crime exist.\textsuperscript{17}

\textsuperscript{12} *Annual datas on cyber crime* furnished by State Crime Record Bureau, Tamil Nadu Police for the year 2008.
\textsuperscript{13} *Ibid.*, for the year 2009.
\textsuperscript{14} www.cbcid.tn.nic.in browsed on 25\textsuperscript{th} December 2010.
\textsuperscript{15} Government of Tamil Nadu G.O.(Ms) No.940, Home (Pol.XII) Department dated 3\textsuperscript{rd} October 2002.
\textsuperscript{16} Government of Tamil Nadu G.O.(Ms) No.226, Home (Pol.XIV) Department dated 18\textsuperscript{th} February 2004.
\textsuperscript{17} www.cbcid.tn.nic.in browsed on 25\textsuperscript{th} December 2010.
Cyber Crime Cases handled by Crime Branch C.I.D., Tamil Nadu Police

Since the inception of Cyber Crime Cell in Crime Branch C.I.D. in the year 2003, the three cases were registered in 2004, one in 2005, one in 2006, eleven in 2007, twelve in 2008 and also twelve cases registered in 2009. Likewise, two cases were detected in 2004, one in 2005, one in 2006, five in 2007, four in 2008 and also four cases were detected in 2009. Four persons were arrested in 2004, three in 2005, one in 2006, five in 2007, four in 2008 and also four persons were arrested in 2009. Whereas, the number of case disposed in court from 2004 to 2009 was only one, that too in the year 2009.18

The overall details of disposal of cyber crimes in the Courts in respect of Tamil Nadu could not be obtained.

COMPARISON OF CASES REGISTERED
(UNDER I.T. ACT AND IPC) - YEARWISE

<table>
<thead>
<tr>
<th>Year</th>
<th>No. of Cases registered and IPCs</th>
</tr>
</thead>
<tbody>
<tr>
<td>2000</td>
<td>40</td>
</tr>
<tr>
<td>2001</td>
<td>35</td>
</tr>
<tr>
<td>2002</td>
<td>30</td>
</tr>
<tr>
<td>2003</td>
<td>25</td>
</tr>
</tbody>
</table>

From 2000 to 2009, 143 cyber crimes were reported in Tamil Nadu. 106 cases were related to IT Act, 2000 and 37 cases were related to IPC sections. Of the total 106 cases registered under IT Act for the year from 2000 to 2009, 37 related to hacking. There were 31 cases of cyber pornography. 13 cases of Tampering, Hacking (10), Threatening E-mail (3), Breach of confidentiality (2), Software Piracy (2), Unauthorised access (1) and Fraud Digital Signature Certificate (1). Of the 37 cases registered for cyber crimes under IPC, 16 cases were related to Criminal Breach of Trust or Fraud, Forgery (16), Creating false information through computer (2), Misappropriation of funds (2) and Fictitious trading account (1).

**COMPARISON OF CASES REGISTERED UNDER I.T. ACT - YEARWISE**
Loss/Damage to computer under IT Act

It is clear from the above data that particularly in 2005 as highest as 15 cases were registered under Loss/Damage to computer. Likewise in the years 2004 and 2007, 7 cases each were registered under Obscene publication/cyber pornography. Out of 37 cyber crime cases registered under IPC, in 2009 as high as 11 cases were registered under Criminal breach of trust and 8 cases were registered under Forgery.

There was an increase in the incidence of the offence under Loss/Damage to computer from 2004 (5), 2005 (15), and decrease in 2006 (7), 2008 (4) and 2009 (3) under the same category.
Likewise in the cases under Obscene publication/cyber pornography, there is fluctuation during the period from 2001 to 2009 except in 2002 i.e.; [2001 (1), 2003 (3), 2004 (7), 2005 (5), 2006 (1), 2007 (7), 2008 (4) and 2009 (3)].
From the above, it is crystal clear that the major number of cases registered under IT Act were established under Loss/Damage to computer, Obscene publication/cyber pornography, Tampering and Hacking. Likewise the major cases were registered under IPC section under Forgery and Criminal breach of trust.

Out of 53 cases of hacking during the above period, 28 cases were registered by Chennai City followed by CB-CID (18 cases), Coimbatore City (6 cases) and Chennai Suburban (1 case). Likewise out of 31 cases of Obscene publication, 18 cases were registered by registered by Chennai City followed by CB-CID (10 cases), Madurai City, Karur and Tiruvallur (1 case each).
The cases registered under IT Act in the above period was 106. Number of Loss/Damage to computer, Obscene publication/cyber pornography, Tampering and Hacking alone totalled to 97 with a percentile of 91.51. Likewise the cases registered under IPC in the above period was 37 in which, Forgery and Criminal breach of trust alone totalled 32 with a percentile of 22.38%. Hence, in the above six heads, 90.21% of the cyber crimes was recorded.
Forgery was recorded in 2000 (4), 2008 (4) and 2009 (8). Likewise Criminal breach of trust was reported in the years 2007 (5) and 2009 (11).
It is also known from the above data that particularly in 2009, 11 cases were registered under Criminal breach of trust and 8 cases were registered under Forgery. Out of 16 cases of Criminal breach of trust, 15 cases were registered by Chennai City followed by Coimbatore City (1 case). Likewise out of 16 cases of Forgery through computer, 11 cases were registered by Chennai City followed by CB-CID (3 cases) and Coimbatore City (2 cases).

Overall, there were 143 cases of cyber crimes from 2000 to 2009, six offences took a major share under IT Act and IPC with 129 cases with a percentile of 90.21. They are Loss/Damages to computer (43 cases with a percentile of 30.07), Obscene publication/cyber pornography (31 – 21.68%), Tampering (13 – 9.09%), Hacking (10 – 6.99%), Forgery (16 – 11.19%) and Criminal breach of trust (16 – 11.19%).

### Persons Arrested on Cyber Crimes in Tamil Nadu

The numbers of persons arrested on cyber crimes in Tamil Nadu has been obtained from the data of National Crime Record Bureau, in which, from the year 2002 to 2009 are only available. The data for the years 2000 and 2001 could not be obtained. Hence, the number of persons arrested has been discussed for the year from 2002 to 2009 are discussed below:

In the year 2002, 2 persons were arrested under I.T. Act in Tamil Nadu. In which, one person was arrested between the age of 18 and 30 years and one person between 30 and 45 years.

In 2003, 6 persons were arrested under I.T. Act and all of them between the age of 30 and 45 years.
In 2004, 16 persons were arrested under I.T. Act, in which, 13 persons were arrested between the age of 18 and 30 years, 3 persons between 30 and 45 years. In this year, 31 persons were arrested under IPC sections, in which, 7 persons were arrested between the age of 18 and 30 years, 18 persons between 30 and 45, 6 persons were arrested between the age of 45 and 60 years. Totally under IT Act and IPC sections, 47 persons were arrested, in which, 20 persons were arrested between the age of 18 and 30 years, 21 persons between 30 and 45, 6 persons were arrested between the age of 45 and 60 years.

In 2005, 21 persons were arrested under I.T. Act, in which, 16 persons were arrested between the age of 18 and 30 years, 3 persons between 30 and 45 years, 2 persons were arrested between the age of 45 and 60 years.

In 2006, 7 persons were arrested under I.T. Act, in which, 4 persons were arrested between the age of 18 and 30 years, 2 persons between 30 and 45 years, one person was arrested between the age of 45 and 60 years.

In 2007, 8 persons were arrested under I.T. Act, in which, one person was arrested below the age of 18 years, 2 persons between 18 and 30, 3 persons between 30 and 45, one person was arrested between the age of 45 and 60 years.

In 2008, 6 persons were arrested under I.T. Act, in which, 2 persons were arrested between the age of 18 and 30 years, 4 persons between 30 and 45 years.

In 2009, 11 persons were arrested under I.T. Act, in which, 5 persons were arrested between the age of 18 and 30 years, 4 persons between 30 and 45, one person between 45 and 60, one person was arrested above 60 years. In this year, 5 persons were arrested under IPC sections, in which, one person was arrested between the age of 18 and 30 years, 2 persons between 30 and 45, 2 persons were arrested between the age of 45 and 60 years. Totally under IT Act and IPC sections, 16 persons were arrested, in which, 6 persons were arrested between the
age of 18 and 30 years, 6 persons between 30 and 45, 3 persons between 45 and 60, one person was arrested above the age of 60 years.

From the year 2002 to 2009, 77 persons were arrested in India under I.T. Act, in which, one person was arrested below the age of 18 years, 43 persons between 18 and 30 years, 26 persons between 30 and 45 years, 5 persons between 45 and 60 years, one person was arrested above the age of 60 years.
Likewise, under IPC sections, 36 persons were arrested. In which, age between 18 and 30, 8 persons were arrested, between 30 and 45, 20 persons were arrested and between 45 and 60, 8 persons were arrested.
From the year 2002 to 2009, totally under IT Act and IPC sections, 113 persons were arrested, in which, 2 persons were arrested below the age of 18 years, 51 persons between 18 and 30 years, 46 persons between 30 and 45 years, 13 persons between 45 and 60, one person was arrested above the age of 60 years.

Through the above data, from the age of 18 to 45 years, 97 persons were arrested out of 113 overall arrested. Hence, 85% of persons have committed cyber crimes in Tamil Nadu between the age of 18 and 45.

**Tamil Nadu Police Academy**

Tamil Nadu Police Academy situated at Oonamanchery, Chennai, has been in the forefront in developing skills of police officers in investigating cyber crimes. The Academy has trained more than a thousand police officers in the advanced skills needed for the investigation of cyber crimes.

**Computer Forensic Laboratory**

In Tamil Nadu, the Forensic Science Department has set up a Computer Forensic Cyber Lab and the lab is having the following softwares: 1) Encase Version-6, 2) Neo Trace Express/Visual Route and Quick View Plus, 3) PDA Seizure Tool Kit, 4) Paraben P2 Explorer, 5) External CD writer, 6) IDE – ATA Writer Blocker, 7) IDE – SATA Writer Blocker, 8) SCSI Writer Blocker, 9) USB Writer Blocker, 10) Skimmers, 11) Mobile Forensic Workstation – Logicube Portable+, 12) Imaging Device – Logicube Talon – Combined unit as Combo, 13) Write block memory card reader, 14) All in one memory card reader, 15) Advance Forensic Work Station – DIBS, 16) Mobile Forensic Forensic Work Station –

---

DIBS, and 17) Imaging Device – DIBS – Raid. I.Os can make use of this lab in the cyber crime investigation.20

As per the Circular Memorandum of the Director General of Police, Tamil Nadu, communicated to the Superintendents of Police of all Districts including Railways and all Commissioners of Police except Chennai, the cyber crime offences of Cheating (Online Lottery and Job Racketing) and Phishing (Net Banking Frauds) have to be investigated by District Crime Branch/Central Crime Branch of respective Districts/Cities. In this regard, the following advices have been given:21

In order to prevent computer crimes and create awareness among Internet users, the CB-CID has collaborated with NASSCOM (a non-profit representative body of Software and Service Companies) and organised two ‘Cyber Safe Chennai Weeks’ in 2008 and 2009 so as to impart training to the police officers for effective investigation of cyber crimes. The CB-CID officials have also contributed to public awareness by displaying posters at the Tamil Nadu Police Stall during the Annual Trade Fair organised by the Government of Tamil Nadu.22

**Infrastructure**

Hardware23 such as six Computers including one server, one Laptop, six UPS, three Printers, eight Cameras including seven Handycam, one Roller palm printer, one Digital Video recorder and 5 Digital Diaries and Software viz. two Operation Software, five Application Software and Utility Software such as

---

20 www.cbcid.tn.nic.in browsed on 15th February 2011.
21 Circular Memorandum of the Director General of Police, Tamil Nadu, Chennai -4 dated 23rd February 2012.
thirteen Personal firewall (Norton), one Winproxy 5.X (10 user), one Encase version 4 and one Advanced Password Recovery Kit, Sharp LCD Projector are provided to the Cyber Crime Cell from the Hardware and Software purchased under Modernisation of Police Force Scheme.\textsuperscript{24} One Digital Presenter was provided.\textsuperscript{25} Fast Bloc Advanced Computer Forensic Data Acquisition hardware Tool and Paraben Forensic USA Cell Phone Seizure Software & Cell Phone Seizure Tool Box were purchased under MPF scheme.\textsuperscript{26}

For tracing cyber crimes, modern laboratory equipments for the value of Rs.70 Lakhs were purchased from America and Israel. New lab was started to function for Chennai Police on 14\textsuperscript{th} August 2009. There are special practices being given to police officials for tracing cyber crimes. Mumbai and Delhi police department were provided with instruments to trace cyber crimes. Special Lab for Cyber Crime Cell was formed in Chennai Police office. For this, 5 Sub Inspectors were appointed. This lab was inaugurated by Commissioner of Police Mr.Rajendran. Special Team was formed under the head of Assistant Commissioner of Police Mr.Sudhakar.\textsuperscript{27}

Sanctions were accorded from Government of Tamil Nadu to form Cyber Crime Cells for Salem and Tirunelveli Cities and to form Cyber Cell Labs for these two cyber cells as well as the existing ones at Coimbatore, Madurai and Trichy. For this, an amount of Rs.16,51,650/- was allotted to each cyber crime cell to procure the materials for Disk Forensics, Mobile Forensic tool kit, High end

\textsuperscript{24} Government of Tamil Nadu G.O.(D) No.143 Home (Modern) Department dated 6\textsuperscript{th} February 2004.
\textsuperscript{25} Government of Tamil Nadu G.O.(3D) No.621 Home/Modern dated 28\textsuperscript{th} June 2005 and G.O.(D) No.445 Home/Modern dated 11\textsuperscript{th} April 2007.
\textsuperscript{26} Government of Tamil Nadu G.O.(D) No.1118, H(M) Department dated 12\textsuperscript{th} September 2007.
\textsuperscript{27} Dinakaran Tamil daily newspaper dated 14\textsuperscript{th} August 2009, p.2.
forensic work station, CDR analyzer, cyber investigation tool kit for E-mail analysis and Network sessions analysis and general tool kit. An amount of Rs.1,02,240/- was allotted for creation of Cyber Crime cells at Salem and Tirunelveli Cities. An amount of Rs.5,69,000/- was allotted to these cyber crime cells for purchasing furnitures.\textsuperscript{28}

The Cyber Crime Cells would run with the strength of one Inspector of Police, one Sub-Inspector of Police, four Other Ranks (Head Constables/Grade.I Police Constables).

\textsuperscript{28} Government of Tamil Nadu G.O.Ms.No.508 of Home (Pol.VIII) Department, dated 14-09-2011

A Cyber Crime Cell was started by Mr.Shailesh Kumar Yadav, Commissioner of Police, Trichy City Police, with the laboratory provided with disk forensics, mobile forensic tool and cyber investigation tool kit for securing protection against rising incidences of cyber crimes including e-mail threat,
phishing, online fraud, copyright infringement, recording and software piracy, cyber stalking and sex-related offences, obscene SMS, currency and document counterfeiting, spoofing, hacking, and virus dissemination.

**Data Security Policy of Government of Tamil Nadu**

The Government of Tamil Nadu will formulate a comprehensive data security policy. Steps are taken to strengthen the Cyber Crimes Cell and sensitize the stakeholders on various aspects of cyber crime.\(^{29}\) Government of Tamil Nadu has taken necessary steps to achieve the mission set forth in this policy, by creating a knowledge drive ecosystem, leveraging entrepreneurship.

**Information Technology Policy for the year 2002**

Tamil Nadu was amongst the first state to come out with an IT Policy.\(^{30}\) With the passage of time and the immense changes that have taken place in technology, it was felt that a new IT Policy is not only necessary, but also essential to take Tamil Nadu to attain a prominent position in IT.

Accordingly, a new IT Policy 2002 was framed to put the ‘smile of prosperity on the face of every citizen of Tamil Nadu by leveraging Information Technology to create value and wealth for a knowledge based state’.\(^{31}\)

The objectives of the policy are:

1. To establish Tamil Nadu as the Destination Choice for IT investments.


2. To upgrade the quality of life for the citizens through e-Governance and IT applications in Government.

3. To empower people in the rural areas so as to bridge the Digital Divide.

4. To develop Research and Development activities.

5. To promote use of Tamil in Information Technology.\textsuperscript{32}

\textbf{Information Communication Technology (ICT) Policy 2008}

Tamil Nadu has been amongst the top three States in terms of Information Communication Technology investments and production. The number of Indian and Multinational organizations having presence in Tamil Nadu is a testimony to this. ICT production in Tamil Nadu touched a high of US $5.7 billion in 2006-07.\textsuperscript{33}

Mr. S. Balu, Retired Deputy Superintendent of Police, who served in Cyber Crime Cell, Chennai City and CB-CID, has investigated more than 60 cyber crime cases and was awarded National Cyber Crime Investigation Award for the year 2005. He said that awareness was to be created for the victim to avoid negligence. There is need to educate the internet users about cyber safety and guidelines to be issued. Due to delayed reporting, there is a difficulty in collecting evidence. Even after one year, action was taken on complaint given. CCTV surveillance and computer log system was to be followed. First case was registered against Dr. Prakash for pornography under I.T. Act in the year 2001.\textsuperscript{34}

\begin{flushleft}
\textsuperscript{32} www.tn.gov.in/documents/policies
\textsuperscript{34} \textbf{Interview with Mr. S. Balu}, Retired Deputy Superintendent of Police, Cyber Crime Cell, Chennai City and CB-CID on 14\textsuperscript{th} October 2013.
\end{flushleft}
NASSCOM’s Cyber Lab was established in Chennai on 29-08-2010. In this lab, 126 security professionals are members.

Department of Information Technology, Ministry of Communication and Information Technology has entrusted NASSCOM-DSCI with the responsibility of implementing the Cyber Security Awareness Project in the public private partnership mode. As a part of the awareness campaign, DSCI conducted a series of events. The programmes extensively covered audiences from industry sectors like IT/BPO, manufacturing, e-commerce, e-governance, telecom, banks, insurance and financial institutions, Public Sector Units, law enforcement agencies like Police & Judiciary, Academia, Government, schools and colleges.35

The battle against cyber crimes must be waged on many fronts. Technological and non-technological measures can reduce the externality effects. At micro level, technological and behavioral factors should be considered in design and implementation of computer networks to provide negative cognitive feedback to cyber criminals. Technological measures range from disconnecting databases containing sensitive information from the internet to the deployment of sophisticated anti-fraud technologies.

**Private School Staff held for Sending Obscene Picture to Actress**

Mr.R.Pandian, Sub Divisional Engineer, Marketing, Bharat Sanchar Nigam Limited, Chennai Telephones, who worked previously in Legal Department, had stated that a Service Engineer who used the User Name and Password in the computer of a private school situated at Mayavaram while repairing the BSNL broadband, sent obscene picture through e-mail message

---

35 *Data Protection Outlook 2009-10* published by Data Security Council of India p.15
thrice to a famous actress (Meena) and on this, actress lodged a complaint with Cyber Crime Cell of Chennai City Police. The police officials registered a case and asked for the I.P. address of the sender. Based on that, BSNL, New Delhi provided information through the Legal Department of BSNL and the accused was arrested.36

**Criminals Surveillance through CCTNS System**

CCTNS was introduced nationwide to create the architecture to trace the criminals through networking. Through this facilitated network in the districts of Tamil Nadu, the F.I.R. and case details are being sent to State Data Collection Centre. First case was registered through online from a person of Gandhi Market of Trichy City on 29th August 2013 for loss of his cell phone.37

**Cyber Crime Cell, Crime Branch CID**

The core task of the unit is to prevent and detect cyber crimes that come under the ambit of the Information Technology Act. There has been a steady increase over the years in the number of cases taken up. The unit opened its account with 3 cases in 2004 (this was the year in which the Cyber Cell was notified as a police station) and within three years, it registered as many as 11 cases in 2007, almost a four-fold increase. Due to better awareness and media coverage of excellent detections by this, more and more complaints are being received by the CB-CID. This is evident from the fact that the total number of cases registered by the Cyber Crime Cell in 2009 was 12. However, during this year, 31 cases have already been registered upto 30th November 2010.38

36 *Interview with R.Pandian*, Sub Divisional Engineer, Legal Department, Bharat Sanchar Nigam Limited, Chennai Telephones on 15th February 2011.
37 Dinamalar Tamil daily newspaper dated 1st September 2013, p.14
38 Crime Branch CID – A Retrospect (1906-2010) published by CB-CID, Tamil Nadu Police.
This also confirms the welcome trend that the initial reluctance of the people and the companies to approach police in cyber crimes has come down over the years. This would facilitate in preparing a database of the techniques employed by the criminals, their on-line characteristics and linkages that would provide crucial clues to the law enforcement agencies in solving crimes.

**Certain cyber crimes reported in Tamil Nadu**

**Bank staff held for cyber crime**

An employee of the Bank of India tapped his bank’s computer network and gathered data on all keys, including passwords, by monitoring the CCTV. Finally, he was caught.\(^{39}\)

Nazim Shah, an Iranian hacker, was arrested for utilising computer networks to illegally transfer cash into his account and using ATMs to withdraw cash from the Commercial Bank of China.

MBA graduate Akaash Singh hacked into an ATM facility using a counterfeit card to mop up several lakhs of cash from a Canara Bank branch in Chennai while using a metallic sleeve.\(^{40}\)

**Online Fraudulent Fund Transfer of UTI Bank, Madurai**

This case was registered in Madurai on the basis of a complaint received from Assistant Vice President, UTI Bank, Madurai, about a fraudulent online fund transfer from the savings account of one of their customers. Investigation revealed the complicity of an employee of a courier company to whom the courier parcel of the bank kit containing Net Banking User ID and Password of Savings Account of

\(^{39}\) The Times of India – English daily newspaper dated 12\(^{th}\) November 2003.

\(^{40}\) http://cybercrime.planetindia.net browsed on 14\(^{th}\) November 2015.
the customer concerned was entrusted for handing over to her. He had stealthily noted down these details, hacked into her account, caused wrongful loss to her by purchasing a camera worth Rs.2,038/- online and transferring Rs.950/- to the account of his friend. Both the employee and his friend were arrested and remanded. The charge sheet was filed on 30th September 2004 and the trial is in progress. 

**Hacking of e-mail ID to spread defamatory messages about a company**

The e-mail ID of a Vellore-based businessman was hacked and used for spreading defamatory messages about his company to his clients. A case was registered. The probe by the Cyber Crime Cell identified two engineers of rival firms who had impersonated as the complainant and obtained his password from the service provider. Armed with this information, they had hacked into his e-mail account and sent defamatory messages to his clients that he would be closing his business on account of poor financial condition. Both the accused were arrested and remanded. The case was charged on 21st April 2006 and is pending trial before XI Metropolitan Magistrate Court, Saidapet, Chennai.

**Verdict of CB-CID Court**

One Mr. Sivakumar of Chennai, ran business for chemical for leather with foreign countries including Brazil. In the year 2004, the foreign customers of his company dropped the business with him. A customer of Brazil intimated Sivakumar that an e-mail was received by him from the e-mail ID of Sivakumar that the latter dropped the business. In this regard, Sivakumar lodged a complaint with CB-CID. During the investigation, two brothers by name Ishad Ahamed (44)

---

41 Crime Branch CID – A Retrospect (1906-2010) published by CB-CID, Tamil Nadu Police.
42 Crime Branch CID – A Retrospect (1906-2010) published by CB-CID, Tamil Nadu Police.
and Altaf Ahamed (42) used the e-mail ID of Sivakumar and informed the customers of Sivakumar that the complainant dropped the business. Both of them confessed that they committed this crime due to business competition. The two accused were arrested and charge sheet was filed against them.43

Both the accused were convicted by CB-CID Court. Sub Judge Tr.R.Shankar on 14th August 2013 pronounced the judgment of 2 years RI and Fine of Rs.5,000/- for the offence u/s.419 IPC (Impersonation), 2 years RI and Fine of Rs.20,000/- for the offence u/s.66 of I.T. Act.

**Hacking-Theft of Information from a Software Company**

A former employee of a software company stole its information and executed the work order of one of its clients, that is, Tirupattur Town Co-operative Bank at a lesser price with the connivance of two bank staff. A case was registered under IT Act and IPC. The scrutiny of the suspected storage media led to the detection of the crime. All the three accused, including two bank employees were charged by the Cyber Crime Cell. Trial awaits vacation of stay granted by the Madras High Court.44

**Overseas Online Job Racket – Nigerian Scam**

A resident of Thanjavur received a forwarded mail from one of his relatives in Kuwait about a job offer in a hotel in Canada during October 2005. He along with a few others responded to this bogus e-mail and paid nearly Rs.2.5 Lakhs for securing this job. Later when the fraud came to light, he wanted action against the culprits. A case was registered in Cyber Crime Cell Cr.No.1/2007 u/s.420 IPC. The Header information of the e-mails sent by the accused indicated

---

44 Crime Branch CID – A Retrospect (1906-2010) published by CB-CID, Tamil Nadu Police.
the location of the Internet Service Provider at West Africa. Hence, the user details were sought through Interpol channels. However, in spite of lengthy correspondence and reminders for more than two years, the user details could not be obtained from the ISP. The case was treated as undetected on 30th October 2008.45

**Sending of Obscene e-mails to a Senior Officer**

An IAS officer received some obscene e-mails and lodged a complaint with the Cyber Crime Cell, CB-CID and a case was registered u/s.67 of IT Act 2000. Working on the IP address and other details of the e-mails, the sleuths found out the involvement of one of his disgruntled staff who wanted to vent his anger against him for having dealt with him on a charge. The accused was arrested and charge sheeted.46

**Arrest of Sri Lankan Credit Card Fraudsters**

A gang of Sri Lankan credit card fraudsters was burst in Chennai in June 2006 and might have heralded in a new type of cyber crime. It was reported that the gang of four men was caught with 116 international credit cards, Rs.6.5 Lakhs and 31 stolen passports. They had allegedly stolen credit card information from unsuspecting people in the UK and had managed to manufacture fake cards that would work on Indian ATMs.

All new credit cards in the UK became embedded with Radio Frequency Identification (RFID) chips that contain different pieces of user information, in order to access the account and withdraw cash, the ATMs has to verify both the magnetic strip and the RFID tag. Without this double verification, the ATM will

45 Crime Branch CID – A Retrospect (1906-2010) published by CB-CID, Tamil Nadu Police.
46 Ibid.
confiscate the card, and possibly even notify the police. ATMs in India, however, only verify magnetic strips and have yet to catch up with advances in western technology.

Under the direction of a computer savvy crime boss, the thieves collected credit card numbers from an unscrupulous gas station attendant in London and uploaded the electronic information to the magnetic strips on the back of phone cards. Then they caught a flight to India.

Since the Indian ATMs only had single point verification, the gang was able to exploit the technology gap all across Tamil Nadu and netted a huge sum. They would have gotten away with it, too. The police did not have a clue about what was happening, and it was only when an unusually attentive security guard posted outside an ATM noticed a man withdrawing cash from multiple cards in succession that he was able to tip off the cops.47

**Online Job Racketeering – Nigerian Scam**

A complaint of cheating through spam e-mail promising overseas jobs in a Canadian Cruise line Ship Company at Malaysia was reported to the Cyber Crime Cell in which the complainant was made to deposit nearly Rs.2.5 Lakhs directly in the foreign account of the accused as a processing fee. Since the bogus e-mails had originated from Malaysia, the Czech Republic and the United States, the user details of the IP Addresses were called for through the Interpol channels.48

---

48 *Crime Branch CID – A Retrospect (1906-2010)* published by CB-CID, Tamil Nadu Police.
Online Cheating – Nigerian Scam

A young woman of Madurai became a victim of a Nigerian on-line job racket when she deposited Rs.1.14 Lakhs in the account of Hari Om Enterprises maintained in a branch of the ICICI Bank at Jaipur on the directions of one Egoama George of Nigeria through e-mail and a case was registered. The e-mail in question had originated from abroad and the mastermind managed to escape. However, the account holder, who received the money, was arrested and remanded. He is facing trial at the XI Metropolitan Magistrate Court, Saidapet.49

Phishing – Online Fraudulent Fund Transfer

A case of phishing came to notice when a sum of Rs.2,49,607/- was fraudulently withdrawn from the Axis Bank account of the complainant through an Internet banking transaction without his knowledge by some unknown person on 10th September 2007. Fortunately, the fraud came to be known soon and this money transfer was stopped. A case was registered u/s.66 of IT Act, 420, 379 IPC and investigation was taken up. Since the IP address of the system used for transferring the funds belonged to the foreign Internet Service Providers of the United States and Nigeria, the Interpol was addressed.50

Online Job Racketing – Nigerian Scam

A Salem based youth got a job offer through the Net from Texaco, North Sea UK’s Galley Oil and Gas Field, United Kingdom. Lured by the offer, he deposited an amount equal to nearly Rs.1,51,000/- directly into the account of a foreign bank towards his Immigration processing fee through a branch of the SBI at Salem. However, the promised job never came his way. Based on his

49 Crime Branch CID – A Retrospect (1906-2010) published by CB-CID, Tamil Nadu Police.
50 Ibid.
complaint, a case was registered in Salem City CCB in July 2007 in Cr.No.15/2007 u/s.467, 468 & 471 IPC. Since there was no progress, the case was transferred to the CB-CID by the DGP in August 2008. In spite of good leads being available, the investigation could not proceed further, as the user details could not be obtained from the countries involved such as Nigeria, Romania, Hong Kong, Canada and the United States. The case had to be treated as ‘undetected’ in November 2009.51

**Theft of Confidential Documents by an Ex-employee from a Multi-national Company**

A complaint was received from a multi-national company against one of its ex-employees for having misused the ID and password of another employee and downloaded more than 4,000 confidential documents worth several million dollars. A case was registered u/s.66 of IT Act, 2000, Section 408 IPC. As this act was recorded on the CCTV video file of the company, the accused was arrested immediately and remanded. The sustained investigation led to the detection and seizure of incriminating evidence.52

**Phishing-Online Fraudulent Fund Transfer**

This is a landmark case of online fraudulent fund transfer handled by the CB-CID Cyber Crime Cell in which the Sec.43-A of the new IT Act, 2008 was invoked for the first time in India in September 2007.

One complainant also filed a petition before the Adjudicating Officer under the Information Technology Act. The matter came up before Thiru P.W.D.Davidar, IAS, Adjudicating Officer and Secretary to Government,

---

51 *Crime Branch CID – A Retrospect (1906-2010)* published by CB-CID, Tamil Nadu Police.
Information Technology Department, Government of Tamil Nadu, Chennai. In his judgment delivered on 12th April 2010. Thiru.Davidar directed the respondent, namely, the ICICI Bank, to pay a total sum of Rs.12,85,000/- to the petitioner within 60 days from the date of issue of the judgment. The ICICI bank went for an appeal before the Cyber Appellate Tribunal, New Delhi.\textsuperscript{53}

**Posting of Obscene Profile of a Young Woman on the Net**

The complainant and her family members received a number of obscene phone calls and from one such caller, she came to know that a porn profile was posted in her husband’s name. Based on her complaint, a case in Crime No.4/2007 u/s.67 of IT Act, Sections 469, 509 IPC was registered. The obscene profile was immediately deleted. However, the user details could not be obtained from the foreign ISP.\textsuperscript{54}

**E-mail threat to VVIPs**

A 23-year-old person from Trichy was arrested by the City Cyber Crime Police on 9th August 2007 on charges of sending an e-mail threat to the Chief Minister of Tamil Nadu and his family.\textsuperscript{55}

In another case, the police team investigating the e-mail threat on the lives of the President and the Prime Minister of India prepared a sketch of the suspect, who had sent the email from a cyber cafe in the city.\textsuperscript{56}

**First Case Convicted under I.T. Act in Tamil Nadu and also in India**

The case related to posting of obscene, defamatory and annoying message about a divorcee woman, in the yahoo message group. E-mails were also

\textsuperscript{53} Crime Branch CID – A Retrospect (1906-2010) published by CB-CID, Tamil Nadu Police.

\textsuperscript{54} Ibid.

\textsuperscript{55} The Hindu – English daily newspaper dated 10th August 2007.

\textsuperscript{56} The Hindu – English daily newspaper dated 29th October 2006.
forwarded to the victim for information by the accused through a false e-mail account opened by him in the name of the victim. The posting of the message resulted in annoying phone calls to the lady in the belief that she was soliciting. Based on the complaint made by the victim in February 2004, the Police traced the accused to Mumbai and arrested him. The accused was a known family friend of the victim and was reportedly interested in marrying her. She however married another person. This marriage later ended in divorce and the accused started contacting her once again. On her reluctance to marry him, the accused took up the harassment through the Internet. In March 2004, the charge sheet was filed u/s.67 of Information Technology Act, 2000, 469 and 509 Indian Penal Code. The accused was convicted to undergo 2 years Rigorous Imprisonment and to pay fine of Rs.4,000/- and other IPC sections.57

Well-known Orthopaedist in Chennai got Life

Dr.L. Prakash stood convicted of manipulating his patients in various ways, forcing them to commit sex acts on camera and posting the pictures and videos on the Internet. The 50-year-old doctor landed in the police net in December 2001 when a young man who had acted in one of his porn films lodged a complaint with the police. Apparently, the accused had promised the young man that the movie would be circulated only in select circles abroad and had the shock of his life when he saw himself in a porn video posted on the web. Subsequently police investigations opened up a Pandora’s box. Prakash and his younger brother, settled in the United States, had piled up close to the one lakh shots and video footages, some real and many morphed. They reportedly minted huge money in

57 www.alertindian.com Case No.3 – browsed on 22nd January 2016.
the porn business. The Fast Track Court Judge convicted in February 2008 that the main accused Dr. Prakash was sentenced to life term under Immoral Trafficking Act, Indian Penal Code, Arms Act and Indecent Representation of Women (Prevention) Act.58

**Bomb Threat to Railway Station**

In an interesting case, a bomb threat message in an encrypted form was registered and investigated in the City Cyber Crime Cell U/s.506 (ii), 507 & 509 IPC. On 8th March 2007, an anonymous inland letter was received by Cyber Crime Cell addressed to the Assistant Commissioner of Police, Cyber Crime Cell, Egmore, Chennai-8. The letter announced that there would be a bomb blast in Chennai White House and Railway Station and challenged the cyber cell authorities to trace the author of the message.

The message of the letter posted by the accused is as reproduced below:

“All Alert there will be a bomb blast in Chennai white house and in railway station in this month if you can find it find it. If you find me I can tell you about the Panipat Blast because our team has only done this. I am working in BPO Company Let us play a game if you find me I will gift my wife to you for one day you can use her as you want. Let us play a puzzle if you find my address I will give clue AA”.

---

58 www.alertindian.com Case No.5 – browsed on 22nd January 2016.
The message in the symbol form is decoded from the front “Marlett” and translated as follows:

“ibm has 161811111194 address has 22 pallavia street because my wife has so beautiful bid her body has like bixthi ig aiyoic wait her just call number if you cbi find it 65262123”.

The matter was probed and the address of the person who owned the phone number 65262123 was traced. The number belonged to one Suresh of Perambur. When examined Suresh revealed the fact that he had married Ms. Anitha his erstwhile colleague. Sachin who did not succeed in marrying Anitha, had a grouse against her and therefore sent lascivious letters to Anitha’s parents in the name of Suresh, so that they may avert the marriage of Anitha with Suresh. However, it didn’t happen. In order to avenge Anitha he went to a browsing center in Chennai. The accused Sachin typed the above said message and changed the font and took printout and he pasted it in an inland letter.

The accused Sachin was arrested on 15th March 2007 and on his confession, the police team went to the browsing center and collected the register with customer ID and Address. The original telegraph forms which was filled up by the accused was collected from the Perambur Telegraph Office. The accused was sent to judicial custody.

This case is a fine show of how messages can be encrypted and e-mailed using computers, which cannot be read without decrypting. The use of cyber
forensic tools help the investigating agency to unfold the cyber mystery and catch the cyber criminals.\textsuperscript{59}

**Women held for Cyber Crime**

A 25-year-old woman, who allegedly hacked the e-mail of a man of the Nilgiris District and used his friends’ contact addresses to cheat them of money, was arrested on 2\textsuperscript{nd} June 2008 by the Cyber Crime Cell of Crime Branch CID police.\textsuperscript{60}

With the arrest of Ritu, the police have arrested all four accused in the case and remanded them to judicial custody. Based on a complaint made by S.D.Paul, a resident of Nilgiris District, the CB-CID conducted an investigation. The investigation revealed that Ritu had befriended his wife and got details about his e-mail ID and password. Ritu then created a new e-mail ID and sent it to Mr.Paul’s contacts and friends appealing to them to send her Rs.75,000/- towards medical expenses. One of the victims was Frank D’Souza, a health officer in Kuwait. He was given the bank account details and requested to send the money. When Mr.D’Souza did not deposit the money, the accused requested him to issue a cheque. Police had by then identified the accused who were wanted in an earlier case registered in Bangalore for a similar offence.

Though the police had arrested three of them, Ritu, the prime accused, was absconding. On 2\textsuperscript{nd} June 2008, she was arrested and her seven-month-old baby sent with her to Puzhal prison.

\textsuperscript{59} Article on *Cyber Crime* submitted by Dr.M.Sudhakar, Assistant Commissioner of Police, Cyber Crime Cell, Central Crime Branch, Egmore, Chennai-8.

\textsuperscript{60} The Hindu – English daily newspaper dated 4\textsuperscript{th} June 2008.
Chennai Engineer held for sending email threat to President

Chennai based software engineer Sriram Jagannath working with a leading IT major company in Chennai, was arrested on 15th October 2008 from his T.Nagar residence, for allegedly sending email threat to President Prathibha Patil. Mr. Sriram was 23 year computer programmer. Rashtrapati Bhavan security traced the email to Tamil Nadu. Following this, the Cyber Crime Cell of the Chennai Police had investigated the case and after screening through dozens of Internet Protocol addresses, zeroed on two persons. Sriram admitted to having sent the mail to the President, Sriram had threatened to eliminate the President in the email.61

Phishing of a Password of a Professor

This is a case of password ‘phishing’ in which a university professor was tricked into disclosing his password to a fraudster who sent some fake e-mails to him that mimicked ‘Yahoo’. The fraudster then gained access into his e-mail account, locked it by changing the password and attempted to extracts financial benefits from his contacts. The victim lodged a complaint, after which a case u/s.66 IT Act, 419, 420 r/w.511 IPC was registered. The Header details of the hacker’s e-mails were retrieved and scrutinised. This led to the recovery of the IP addresses of the source computer. Since the Internet Service Provider was traced to be in Nigeria, the Interpol/CBI, New Delhi, was requested to obtain user details from the Interpol, Lagos, at Nigeria. However, inspite of several reminders, no

---

details were received. Under these circumstances, the case was treated as ‘undetected’ on 13th April 2009.62

Impersonation and Money Collection on Net by a Women Hacker

This was an audacious extortion racket by a 25-year-old woman who, while visiting the complainant (a defence officer residing in the Nilgiris District), surfed to peep into his e-mail password and hacked into his account. She circulated fraudulent e-mails to his contacts, seeking financial help from them towards his medical treatment.

One of the friends of the victim, who received this e-mail, alerted him about this cheating game. The victim lodged a complaint on 16th May 2008 with the Cyber Crime Cell, CB-CID, and a case u/s.66 IT Act, 419, 465, 420 r/w.511 IPC was registered.

It was the timely intervention of the CB-CID officials that prevented further damage. The IP address of the accused was tracked right up to her computer and she was arrested at Bangalore along with her husband and two associates. The con woman had a criminal past and was involved in several cases of cheating. After completing the investigation, a charge sheet was filed in the court against all four accused on 30th January 2009. The case is pending trial before the court.63

Hacking of e-mail Account of a Senior Official

A complaint was received from a senior IAS officer that he had received an account alert e-mail from Yahoo! In July 2008, he was requested to furnish his password and other details. Accordingly, he had given the required

---

63 Ibid.
particulars. However, later when he tried to browse his e-mails, he was unable to do so. He then learnt from one of his friends that his e-mail ID had been misused by someone. On his complaint, a case was registered under IT Act on 29th July 2008. Since the IP Address of the hacker belonged to Nigeria, a report was sent to the Interpol/CBI, New Delhi, to obtain the user details from the Nigerian authorities.64

**Online Lottery fraud – Nigerian Scam**

This is one of the rare cases where the police have been successful in arresting Nigerians responsible for a plethora of frauds on the Net. In this case, a Central Government employee residing at Kalpakkam in Kancheepuram District responded to a spam mail purported to have been sent by MSN/Yahoo congratulating him on winning an online lottery worth Rs.4 Crores in December 2007. To claim this lottery prize, he was made to remit an amount of nearly Rs.14.68 Lakhs as service charges on various accounts specified by the accused. However, the dream lottery prize never reached him; even the service charges were not refunded! On his complaint, a case was registered by CB-CID.

The mobile phone calls made by the accused gave very useful leads, after which a CB-CID team visited Mumbai and arrested four Nigerians and two Indians in May 2009. Laptops, mobile phones, SIM cards and other incriminating documents were seized from the accused. With the help of bank authorities, an overall amount of Rs.9 Lakhs was frozen in their accounts.65

---


65 *Crime Branch – A Retrospect (1906-2010)* published by CB-CID, Tamil Nadu Police.
Tamil Writer as Cyber Victim

In the year 2008, by thieving the ID of an email of Mr. Charu Nivethitha, a writer in various Tamil magazines, email was sent to more than 2000 persons wrongly quoted that he was in Malaysia for attending a conference, that he forgottenly left the bag in a taxi which contained money, passport and other important documents, that 3200 dollars (approximately Rs.1,60,000/- in Indian money) was needed for settling hotel bills and for returning to India, that the money might be sent through Western Union Money Transfer. The cyber criminal entered into the mail id in hotmail and rediffmail and changed the password. A complaint was sent to Western Union Money Transfer and effort was taken to block the sending of money to the culprit.66

Online Overseas Job Racket

An unemployed person of Arakkonam searched for an overseas job offer on the Internet and received an offer from the Gallery Hotel, 10, Queenberry, London, UK, and Lufthansa Airlines, Heathrow Airport, UK, through e-mail. Trusting the mail, he paid Rs.1,80,000/- as processing charges and so on and was cheated. Initially, his complaint was registered in July 2009 by the District Crime Branch, Vellore District, in Crime No.21/09 u/s.420 IPC. Subsequently, this case was transferred in Cyber Crime Cell, CB-CID, in November 2009.67

Bangalore Engineer held for Cyber Crime

Social Networking sites seem to be used as a platform for phishers to prey on their targets. The CB-CID arrested two Bangalore-based persons, including an engineer, for their alleged involvement in a Rs.26.55 Lakh net banking fraud.

67 *Crime Branch CID – A Retrospect (1906-2010)* published by CB-CID, Tamil Nadu Police.
The police said R.Suresh Kumar (28) and S.Arun Kumar (23), who served as ‘money mules’ (whose bank accounts are used to transfer money siphoned off online) for cyber criminals, were brought to Chennai and remanded to judicial custody. According to the police, S.Salahudeen, Managing Partner of Trichy-based Ahamed and Company approached the Assistant Director General of Police, CB-CID, on 2nd November 2009 with a complaint that Rs.26.55 Lakhs had been fraudulently transferred from his account through net banking during July and August 2009.

A case was registered under Section 66 of the Information Technology (Amendment) Act, 2008 and IPC Sections 419 and 420 and investigation was begun by the Cyber Crime Cell, CB-CID, Chennai.

The investigation officers, scrutinising the server log of the victims’ bank, found that the hacker had used computer systems connected to the network of internet service providers in Nigeria, Canada. They also found that eight ‘mules’ had been recruited in the country, including in Chennai, Mumbai, Calcutta, Bangalore and Sangli (Maharashtra). “The money is siphoned off by the hackers and transferred to the account of the ‘mules’ who had withdrawn it and remitted it in accounts given by the hackers. They take a commission of 10%” said a CB-CID official. One of the ‘mules’ – C.Sridhar of Porur – who helped transfer Rs.4 Lakhs from Salahudeen’s account was arrested on January 12. Based on information that two other ‘mules’ were in Bangalore, CB-CID Inspector G.Velmurugan rushed there and arrested Suresh Kumar and Arun Kumar who helped in the transfer of Rs.1 Lakh and Rs.3 Lakhs respectively.
The police are now investigating if the hackers stole the identity of Salahudeen for online transaction by phishing email or by planting keylogger software. As of now, Rs.11 Lakhs has been returned to the victims. The CB-CID trying to trace the brains behind the racket, has sought assistance of the Central Bureau of Investigation and the Interpol.68 “The hackers befriend a person either through social networking site or chatting sites. They project themselves as businessmen. After a week, they ask for the bank account number. Lured by the money involved, people become mules. Later, they become enmeshed in a racket” a police official said.

A CB-CID team visited Mumbai and arrested six accused including four Nigerians in May 2009.

**Mumbai Man held in Online Job Racket**

The Cyber Crime Cell of the Tamil Nadu Crime Branch-CID has arrested a 25 year old man for cheating a person of Rs.2 Lakhs by promising job.69 According to the police, V. Rajkumar of Trichy had lodged a complaint stating that he was cheated of Rs.2 Lakhs by an online job racket. In his complaint, he said that in September 2009, he received an e-mail from the ID, UKJobalerty.jobalert@yahoo.co.nz on a vacancy in London hotel. The mail asked him to refer to the website www.brunelhotelondon.co.uk for further details. Rajkumar responded to the e-mail and applied for the post of a supervisor. As instructed by the accused, the complainant deposited Rs.2,06,240/- as visa application fees, insurance charges and basic traveling allowance in three accounts in Mumbai given by the accused. But the job never came through.

---

68 The Times of India – English daily newspaper dated 1st March 2010.
69 The Times of India – English daily newspaper 7th June 2010.
A case was registered with the CB-CID on orders of the ADGP Archana Ramasundaram.

They located one of the beneficiary account holders and the accused Deepak Saini (25) of Mumbai was arrested on June 2. He had been remanded in judicial custody. A mobile phone with memory card and a bank debit card were also seized from the accused.

**Online Lottery Frauds – Nigerian Seams**

A businessman of Conoor, the Nilgiris District, gave a complaint, after which a case was registered in the CB-CID Cyber Crime Cell on 5th September 2009. An SMS sent by some unknown person informed him that he had won 7,50,000 pounds in a lottery and that for making a claim, he should send his personal details to the specified e-mail. Lured by this offer, the complainant and his other family members deposited nearly Rs.14,29,140/- as delivery charges, tax charges, custom settlement and clearing charges into various bank accounts at New Delhi, Jaipur and Meghalaya. Later, they realized that they had been cheated. Investigation is in progress and, wherever required, assistance of other state police is also being sought.

Another online lottery scam was reported by a resident of Theni District who was cheated through an SMS in August 2009 informing him that he had won 8,00,000 pounds in a mobile draw. He deposited nearly Rs.3,55,600/- as various charges in various bank accounts specified by the accused. Yet another case of this type U/s.420, 465, 468, 471 IPC was registered and investigation taken up.
Mirza Sarfraz Baig, one of the accused, was arrested by the CB-CID in Mumbai in May 2010. He was brought to Chennai and remanded.\footnote{Crime Branch CID – A Retrospect (1906-2010) published by CB-CID, Tamil Nadu Police.}

**Online Fraudulent Fund Transfer**

On 26\textsuperscript{th} June 2009, a resident of Cuddalore District, who held an account in the local ICICI Bank, found that a sum of Rs.6 Lakhs had been fraudulently transferred online from his account to another account. A case was registered in Thiruppapuliyur Police Station U/s. 406 IPC, 66 IT Act, and 419, 420 IPC. In March 2010, this case was transferred by the DGP to the Cyber Crime Cell. The CB-CID team visited Ernakulam, Hyderabad and Delhi and arrested five accused.

In the second case, Madurai based Engineer V. Saravanan in August 2009 lodged a complaint with the CB-CID saying that Rs.75,510/- was illegally transferred via net banking from his account, following his response to a phishing e-mail purportedly sent by his bank. He gave his user ID, login password and transaction password. The money was transferred to accounts in New Delhi and Mumbai. Cyber Crime Wing registered a case and a probe began. On May 19, police arrested I.Ibrahim Ansari of Mumbai after finding that he had received Rs.25,000/- from Saravanan’s account on 22\textsuperscript{nd} August 2009.\footnote{Ibid.}

**Man held for Allegedly Harassing Sctress Sneha**

On the complaint of actress Sneha in August 2009, sleuths of the Cyber Crime Cell arrested a Bangalore resident here on Sunday night on charges of sending at least 150 SMS messages to actor Sneha proposing to marry her. The sophisticated Cyber Crime Laboratory that was launched a couple of days ago came handy in cracking the case. According to police sources, Ms. Sneha lodged a
complaint with the Commissioner of Police T. Rajendran that an unidentified man was harassing her by sending repeated messages in the last six months. Deputy Commissioner of Police (Central Crime Branch) C. Sridhar formed a special team led by the Assistant Commissioner of Police (Cyber Crime Cell) M. Sudhakar to investigate the case. The team tracked the mobile number to Bangalore where N. Raghavendran (35), a B.Com. graduate in real estate business, was using it. Though there was no obscenity in the messages, the accused harassed the actor by sending the messages frequently asking her to marry him.

“It appears that he got the mobile phone number of the actor through some friends in the film industry. Even when she changed the number, he managed to get the new one,” Dr. Sudhakar told. Though the actor never responded to his messages, she once replied requesting him not to disturb her. A special team apprehended Raghavendran when he was coming out of a hotel in T. Nagar. He had come to Chennai in connection with a land deal. The accused was arrested under the provisions of the Tamil Nadu Prohibition of Harassment of Women Act and also on charges of causing criminal intimidation. He was produced in a city court and remanded to judicial custody.⁷²

BSNL SIM Card Fraud

Superintendent of Police, Vellore district, has entrusted to the District Crime Branch (DCB), Vellore, the complaint forwarded by the General Manager of the Bharat Sanchar Nigam Limited (BSNL), Vellore Telecom District, about the fraud committed by a customer who purchased Subscriber Identity Module (SIM) cards and absconded after using the same for making international calls

worth Rs. 1.97 crore in the last one-and-a-half months, thus causing a huge loss to the BSNL.  

According to police sources, a company styled as Himalaya Herbal in Sankaranpalayam in Vellore, had purchased 126 SIM cards, out of which 37 had been used for making international calls. The DCB has sought evidence from the BSNL about the fraud in order to facilitate the registration of a case and further investigation.

When asked about the fraud, A. Shajahan, General Manager, BSNL, Vellore, told newsmen here on Monday that the fraud came to light when BSNL authorities who sent bills for payment to the address of the company, found that there was no company by the name Himalaya Herbal in the given address. The customer had purchased the SIM cards under the CUG (closed user group) category. When questioned further about the fraud, Mr. Shajahan refused to divulge the details of the case, on the grounds that it was under police investigation.

The vigilance cell of the BSNL is also making a parallel investigation into the fraud.

**Nigerian National held for Fraud in Coimbatore**

In October 2009, the Crime Branch sleuths of the Coimbatore City Police arrested a Nigerian national Odiegwu Nnamdi Jude on charges of cheating a businessman in Coimbatore.

Mahadevan of Peelamedu engaged in repairing and servicing textile mill machinery received a Short Message Service (SMS) on his phone on September 73 The Hindu – English daily newspaper dated 16th October 2009.
17 stating that he had been chosen for a lottery prize of two lakh pounds. When he responded to the SMS, he was given an e-mail address to contact the processing agent to collect his prize. On sending an e-mail, Mahadevan was asked to remit Rs.31,583 towards processing charges and customs clearance to get the prize money.\(^7\)

Accordingly, the complainant deposited the sum in the account number provided. When the complainant asked for the prize money by sending an e-mail he was asked to immediately come to Mumbai. On reaching Mumbai, when he called the particular mobile number, Mahadevan was asked to remit another Rs.1.05 lakhs said to be for scanning charges. He paid the money and when there was no response from the other end, the complainant turned suspicious and preferred a complaint with the police.

City Police Commissioner, P.Sivanandi ordered for a probe and Deputy Commissioner of Police (Crime and Traffic), N.Kamini constituted special teams led by Assistant Commissioner, M.Selvarajan. The complainant was asked to continue his negotiations with the processing agent. Finally, the agent said that his representative would come to Coimbatore to hand over the money. Immediately a trap was laid and the police waited at Gandhipuram bus stand and nabbed Odiegwu Nnamdi Jude.

Police found a gadget that resembled a phone, a mini locker, bundles of black colour and white colour papers and chemical substances in his luggage. When inquired, the accused said that the chemicals were meant for turning these paper bundles into U.S. dollars. All the recovered from his possession were

\(^7\) The Hindu – English daily newspaper dated 8\(^{th}\) October 2009.
meant for cheating hapless victims lured by such e-mails and SMS. He was taken
into custody and the Police have registered a case against the Nigerian national
under sections 419 and 420 (cheating) of the Indian Penal Code.

Efforts were on to verify the transactions of the bank account, in which
Mahadevan had remitted the money. Police said that the accused nabbed could
just be an agent and there could be a large network operating across the country.
Mr. Sivanandi asked the public to be cautious and not to be lured by such offers of
lottery or prize being intimated through SMS and e-mails. In the event of any such
information, the public should approach the City Crime Branch, he said.

**Chinese held for using Fake Credit Card**

A Chinese settled in Singapore who attempted to purchase gold in a
jewellery shop using a fake credit card was arrested by the Central Crime Branch
police, Chennai on 14th October 2009. According to police sources, a man who
claimed to have come from Singapore gave his credit card to settle a bill in a
jewellery shop in Purasawalkam on Tuesday. However, the Electronic Data
Capturing Machine rejected the transaction. Officials at the Standard Chartered
Bank, being the acquiring bank in this case, found that the actual owner of the
credit card was based in Bangladesh.

Enquiries made with him revealed that he had not come to India and the
credit card was very much with him. On the instructions of the Commissioner of
Police Mr. T. Rajendran, a special team followed specific clues and apprehended
the suspect T. Tankohyu who was staying in a hotel on the Armenian Road.

---

75 The Hindu – English daily newspaper dated 16th October 2009.
The suspect was in possession of four fake credit cards. He claimed to have bought the cards in Malaysia on payment. Two mobile phones were seized from him. On Tuesday night, the Chennai Police arrested a two-member gang and seized 11 fake credit cards. The accused told investigators that a gang based in Malaysia had supplied the credit cards. In another case, a youth who used a fake credit card to purchase gold in a shop at T. Nagar was arrested. The data stored in his card belonged to a person living in the United Kingdom.

**Bank Staff held for Hacking**

One B.S. Sainath Reddy, formerly Assistant Vice President of Axis Bank was arrested for an online fraud in which hacking and siphoning of Rs.27 Lakhs from Axis bank account was carried out. Three other people were arrested previously in the case.76

Police began investigation into this case after a businessman in Tamil Nadu complained that money had been siphoned out of his bank account. The funds were withdrawn in 19 transactions between 20th July 2009 and 13th August 2009.

Reddy is alleged to have siphoned out Rs.5 Lakhs from the compromised account from a computer at his residence. The police have traced an IP address used by the accused. The remaining amount was transferred through online by the hackers logging into the compromised account in a short span of time from various locations around the world including Nigeria and Canada. The other three hackers arrested previously had said that they had transferred funds to accounts at the instructions of unknown persons from whom they received a commission.

---

2 Men held for Stealing via Net Banking

The CB-CID’s Cyber Crime Wing on 22nd May 2010 arrested two Mumbai men for withdrawing Rs.26.55 Lakhs and Rs.75,510/- respectively through fraudulent means from two separate accounts of two Tamil Nadu based persons using net banking. The arrest, S.Vinayak Shivaji Khandare (20) and I.Ibrahim Ansari (25) have been brought to Chennai and remanded in judicial custody at the Puzhal Prison.  

On 5th November 2009, Trichy based businessman S.Salahudeen from Trichy noticed an illegal transaction from his account through net banking and alerted the police and bank officials, the police said. The transaction was found to be done by couriers. Cyber Cell officials found involvement of eight couriers in Chennai, Mumbai, Kolkata, Bangalore and Sangli in Maharashtra.

The couriers would withdraw the amount and deposit it in accounts given by hackers after deducting their 8-10% commission. The CB-CID arrested C.Sridhar of Chennai, R.Suresh Ramdas and S.Arun Kumar of Bangalore in January and February 2010. In March, they arrested one of the prime accused, B.S.Sainath Reddy at Hyderabad. On May 17, a police team went to Mumbai and nabbed Khandare. He confessed that he received Rs.50,000/- from the account of the complainant.

In the second case, Madurai based Engineer V.Saravanan in August 2009 lodged a complaint with the CB-CID saying that Rs.75,510/- was illegally transferred via net banking from his account, following his response to a phishing e-mail purportedly sent by his bank. He gave his user ids, login password and

---

transaction password. The money was transferred to accounts in New Delhi and
Mumbai. Cyber Crime Wing registered a case and a probe began. On May 19,
police arrested I.Ibrahim Ansari of Mumbai after finding that he had received
Rs.25,000/- from Saravanan’s account on 22nd August 2009.

A police officer said: “Hackers steal the id and passwords of victims either
by phishing email or by planting malicious software. They recruit accomplices or
couriers through social networking sites. They then get details of the couriers and
transfer victims’ money. They withdraw from these accounts a share after paying
commission to the couriers”.

Some Tamil Movies on Cyber Crime

Unnai Pol Oruvan

This movie was released in the year 2009. In this movie, the hero
Kamalhaasan is a anonymous caller demands Police Commissioner to release
militants in exchange for information about many bombs planted across Chennai
City. The hero for killing the terrorists who under police custody, is using
advanced software to automatically switch the numbers and locations of his
mobile phone SIM cards every minute, which prompting the Police Department to
employ the services of hacker. However, the hacker found the location.

Enthiran

This is a 2010 Tamil Science fiction film acted by Rajinikanth. The story
revolves around a scientist’s struggle to control his creation, an android whose
software is upgraded to give it the ability to comprehend and exhibit human
emotions. The project backfires when the robot falls in love with the scientist’s
girl friend and is manipulated by a rival scientist into becoming homicidal. The
robot denied to obey the scientist and did untoward activities which causes public disaster. The hero finally got controlling the robot and dismantled it.

**Naanayam**

This is a 2010 Tamil film. In this movie, a bank promotes its new branch as the World’s Safest Bank with the security lock through four leveled locking system vault which was designed by the hero Prasanna. He was netted by a gang to rob that bank by blackmailing and threatening in some aspects. The hero and the gang entered the vault by violating computer security and when attempting rob, the hero manages to escape by locking the robbery gang inside the vault. Finally the vault was saved from the theft.

**Sigaram Thodu**

This Tamil movie was released in the year 2014. The hero Vikram Prabhu who is a Sub Inspector of Police. In that movie, an employee of private bank assisted by his friend withdrew the amount ATMs by using fake card which was created with the database of banks. They also planned to steal money by using information from international credit cards and the same was carried out. The hero however nabbed them.

**Baabanasam**

This is a 2015 Tamil thriller film in which the hero Mr.Kamalhaasan’s daughter while attending nature camp, she was videographer in the bathroom by a hidden cell phone. The culprit was accidentally killed by hero’s wife and daughter when he blackmailed them if the vide would be uploaded in the internet unless they would sexual favour for him.