**Selected Case Studies on Cyber Crime**

1. [Selected Case Studies on Cyber Crime](http://satheeshgnair.blogspot.com/#Selected_Case_Studies_on_Cyber)
   1. [Preview](http://satheeshgnair.blogspot.com/#Preview_6452957224100828_36492_5930722393095493)
   2. [Introduction](http://satheeshgnair.blogspot.com/#Introduction_27793284971266985_5248389532789588)
   3. [Taxonomy](http://satheeshgnair.blogspot.com/#Taxonomy_24259919207543135_030_9210952194407582)
   4. [Theft Of Services](http://satheeshgnair.blogspot.com/#Theft_Of_Services_465713580138)
   5. [Computer Intrusions](http://satheeshgnair.blogspot.com/#Computer_Intrusions_9647361049)
   6. [Computer Viruses, Worms, Trojan Horses, Spy-ware and Other Mal-ware](http://satheeshgnair.blogspot.com/#Computer_Viruses_Worms_Trojan_)
   7. [Distributed Denial of Service Attacks](http://satheeshgnair.blogspot.com/#Distributed_Denial_of_Service_)
   8. [Internet Auction Fraud](http://satheeshgnair.blogspot.com/#Internet_Auction_Fraud_2322764)
   9. [Pay-Per Click Fraud](http://satheeshgnair.blogspot.com/#Pay_Per_Click_Fraud_2088293200)
   10. [Nigerian Advance Fee Fraud](http://satheeshgnair.blogspot.com/#Nigerian_Advance_Fee_Fraud_235)
   11. [Reshipping Fraud](http://satheeshgnair.blogspot.com/#Reshipping_Fraud_3077056575566)
   12. [High Yield investment programs](http://satheeshgnair.blogspot.com/#High_Yield_investment_programs)
   13. [Diploma Scam](http://satheeshgnair.blogspot.com/#Diploma_Scam_27387002296745777_6291344063356519)
   14. [Free Product and Service offers](http://satheeshgnair.blogspot.com/#Free_Product_and_Service_offer)
   15. [Bogus Diet Patches](http://satheeshgnair.blogspot.com/#Bogus_Diet_Patches_96301265154)
   16. [Phishing, Carding, and Money Laundering](http://satheeshgnair.blogspot.com/#Phishing_Carding_and_Money_Lau)
   17. [Pumping and Dump Stock Fraud](http://satheeshgnair.blogspot.com/#Pumping_and_Dump_Stock_Fraud_1)
   18. [Spam](http://satheeshgnair.blogspot.com/#Spam_38594176061451435_4144763_19743805285543203)
   19. [Scheduled Controlled Substances Sold Online without prescription](http://satheeshgnair.blogspot.com/#Scheduled_Controlled_Substance)
   20. [Child Exploitation/ Child Pornography and illegal Obscenity](http://satheeshgnair.blogspot.com/#Child_Exploitation_Child_Porno)
   21. [Warez](http://satheeshgnair.blogspot.com/#Warez_18427631445229053_274137_7960434053093195)
   22. [Online Sale of Replica Counterfeit Trademarked Product](http://satheeshgnair.blogspot.com/#Online_Sale_of_Replica_Counter)
   23. [Untaxed Cigarettes Sold over the Internet](http://satheeshgnair.blogspot.com/#Untaxed_Cigarettes_Sold_over_t)
   24. [Online Gambling](http://satheeshgnair.blogspot.com/#Online_Gambling_40621191170066)
2. [Cyber Crime in India: Case Studies](http://satheeshgnair.blogspot.com/#Cyber_Crime_in_India_Case_Stud)
   1. [Insulting Images of Warrior Shivaji on Google - Orkut](http://satheeshgnair.blogspot.com/#Insulting_Images_of_Warroir_Sh)
      1. [How does Google, India respond?](http://satheeshgnair.blogspot.com/#How_does_Google_India_respond_)
      2. [How does it Airtel react to rectify its mistake?](http://satheeshgnair.blogspot.com/#How_does_it_Airtel_react_to_re)
      3. [What is the current Scenario?](http://satheeshgnair.blogspot.com/#What_is_the_current_Scenario_1)
   2. [Kenneth L. Haywood](http://satheeshgnair.blogspot.com/#Kenneth_L_Haywood_424762024544)
   3. [Financial crimes](http://satheeshgnair.blogspot.com/#Financial_crimes_3199138725176)
   4. [Cyber pornography](http://satheeshgnair.blogspot.com/#Cyber_pornography_166639020666)
   5. [Online gambling](http://satheeshgnair.blogspot.com/#Online_gambling_27115937881171)
   6. [Intellectual Property crimes](http://satheeshgnair.blogspot.com/#Intellectual_Property_crimes_0)
   7. [Email spoofing](http://satheeshgnair.blogspot.com/#Email_spoofing_329149830155074)
   8. [Cyber Defamation](http://satheeshgnair.blogspot.com/#Cyber_Defamation_5085104554891)
   9. [Cyber stalking](http://satheeshgnair.blogspot.com/#Cyber_stalking_838339143432676)
   10. [Unauthorized access to computer systems or networks](http://satheeshgnair.blogspot.com/#Unauthorized_access_to_compute)
   11. [IPR Theft](http://satheeshgnair.blogspot.com/#IPR_Teft_887308968231082_60541_7121198000386357)
   12. [Email bombing (DoS)](http://satheeshgnair.blogspot.com/#Email_bombing_DoS_171188047155)
   13. [Data diddling](http://satheeshgnair.blogspot.com/#Data_diddling_3774617835879326_04138104058802128)
   14. [Internet time theft](http://satheeshgnair.blogspot.com/#Internet_time_theft_0883224243)
   15. [SBI arm wins cybersquatting case - Peeyush Agnihotri - Tribune News Service](http://satheeshgnair.blogspot.com/#SBI_arm_wins_cybersquatting_ca)
   16. [Credit Card Frauds](http://satheeshgnair.blogspot.com/#Credit_Card_Frauds_57977316156)
       1. [Three-in-one fraudster](http://satheeshgnair.blogspot.com/#Three_in_one_fraudster_7837918)
       2. [Trapped](http://satheeshgnair.blogspot.com/#Trapped_7527636215090752_54535_3676432864740491)
   17. [India's First ATM Card Fraud](http://satheeshgnair.blogspot.com/#India_s_First_ATM_Card_Fraud_0)
   18. [Work at Home scams Exposed](http://satheeshgnair.blogspot.com/#Work_at_Home_scams_Exposed_652)
   19. [Case of Cyber Extortion](http://satheeshgnair.blogspot.com/#Case_of_Cyber_Extortion_073842)
   20. [ICICI Bank Phishing](http://satheeshgnair.blogspot.com/#ICICI_Bank_Phishing_9818138880)
   21. [Cyber Lotto an Effective Tool of Frauds](http://satheeshgnair.blogspot.com/#Cyber_Lotto_an_Effective_Tool_)
   22. [Collective Scam in Call Center](http://satheeshgnair.blogspot.com/#Collective_Scam_in_Call_Center)
   23. [Reliance made to pay the Consumer](http://satheeshgnair.blogspot.com/#Reliance_made_to_pay_the_Consu)
   24. [Pune BPO-Scam](http://satheeshgnair.blogspot.com/#Pune_BPO_Scam_708848194219172__588504483923316)
   25. [Gurgaon BPO Scam](http://satheeshgnair.blogspot.com/#Gurgaon_BPO_Scam_4460621122270)
   26. [Bangalore BPO Scam](http://satheeshgnair.blogspot.com/#Bangalore_BPO_Scam_05699411500)
   27. [Data theft makes IT firm quit India](http://satheeshgnair.blogspot.com/#Data_theft_makes_IT_firm_quit_)
   28. [Government and Defense sites Attacked and used](http://satheeshgnair.blogspot.com/#Government_and_Defense_sites_A)
       1. [Similar instances](http://satheeshgnair.blogspot.com/#Similar_instances_598498154431)
3. [Cyber Crime Convictions & Judgments](http://satheeshgnair.blogspot.com/#Cyber_Crime_Convictions_Judgme)
   1. [Case 1: First  
      conviction in India](http://satheeshgnair.blogspot.com/#Case_1_First_conviction_in_Ind)
   2. [Case-2: First juvenile accused in a cyber crime case.](http://satheeshgnair.blogspot.com/#Case_2_First_juvenile_accused_)
   3. [Case 3: First case convicted under Information Technology Act 2000 of India.](http://satheeshgnair.blogspot.com/#Case_3_First_case_convicted_un)
   4. [Case 4: Father & son convicted under IT act in Kerala.](http://satheeshgnair.blogspot.com/#Case_4_Father_son_convicted_un)
   5. [Case 5: Well-known orthopedist in Chennai got life.](http://satheeshgnair.blogspot.com/#Case_5_Well_known_orthopedist_)
   6. [Case 6:Juvenile found guilty for sending threatening email.](http://satheeshgnair.blogspot.com/#Case_6_Juvenile_found_guilty_f)

**Preview**

When we are talking about a subject as broad as case studies on cyber crime it's helpful to have a clear structure. Since this paper is being presented to the delegates of Southern Regional Workshop On Cyber LAW with an emphasis on "Issues and Challenges in Enforcement". I am focusing on the issue more from a national level although an international perspective for the subject is observed and adopted where relevant. The way I have approached and classified the subject, in better words the taxonomy of this paper can be observed as (1) Crimes that focus on tangible networks and hardware, (2) Fraud & Deceptive Crimes and (3) Online Crimes.

Now let me give you an overview of certain terms which are regularly used in the Cyber Crime world before I start talking about the examples. I am sure many of you would know this and there are a lot of new terms being introduced every day I am sure this could be a starting point.

|  |  |
| --- | --- |
| Threat Name | What is means? |
| Mal-ware | Infection to the systems by viruses, worms, Trojans or spy-ware |
| Phishing | Impersonation of the organisation by email or any other electronic means |
| Spam | Unsolicited email messages |
| Denial-of-Service | Attempt to overwhelm or overload the organizations website, network by which it becomes unavailable to the outside world |
| Unauthorised Access | Unauthorised access of systems resources by outsiders |
| Vandalism/ Sabotage | Destruction or damage to organizations systems |
| Extortion | Demands for money or other concessions based on threats |
| Fraudulent Transactions | Transaction that result loss to the organisation or its customers |
| Physical Loss | Loss or theft of computers or physical storage media |
| Unauthorised by Insiders | Successful access by insiders to unauthorised data |
| Insider Misuse | Unauthorised usage by insider by violating the security polices of the organisation |

As you can see from the classification Cyber crime can evolve from various areas. When we consider elements that support cyber crime from 'insider', it can be viewed as portable storage misuse, unnecessary software download, illegal p2p file sharing, misuse of remote access programs, rogue wifi-access points, rogue modems, media downloading, personal devices, unauthorised blogging, personal instant messaging accounts, message board posting, personal email accounts, non-network web browsing and business email misuse.

While I have covered almost all types of Cyber crime examples I have not included examples of cyber war, espionage and terrorism since I feel it is out of scope for this paper. However I would be happy to discuss these topics if any of you readers are interested

**Introduction**

Today Cyber crime is no longer the domain of high school hackers but is populated by organized criminals, unfriendly nation states and terrorists. The problems we face are far more severe than compromised personal data. Our physical security is threatened by vulnerabilities in our electronic information systems.

Now I am quoting here a news article from a very popular internet site, which has a statement from David DeWalt CEO of McAfee as it clearly depicts one of the real challenges in the enforcement of Cyber Law. It reads as "Citing recent highly publicized corporate data breaches that have beset major companies like Ameritrade, Citigroup, and Bank of America, McAfee CEO David DeWalt, said that cyber-crime has become a **US$105 billion business** that now surpasses the value of the illegal drug trade worldwide.

Despite the increase in government compliance requirements and the proliferation of security tools, companies continue to underestimate the threat from phishing, data loss, and other cyber vulnerabilities, DeWalt said. 'Worldwide data losses now represent US$40 billion in losses to affected companies and individuals each year, DeWalt says. But law enforcement's ability to find, prosecute, and punish criminals in cyberspace has not kept up: "If you rob a 7-11 you'll get a much harsher punishment than if you stole millions online," DeWalt remarked. "The cross-border sophistication in tracking and arresting cyber-criminals is just not there."'" [1](http://satheeshgnair.blogspot.com/#FOOTNOTE-1)

Well DeWalt's comment is not just a representation of what is happening in the West or Far East it is a global issue. The challenges in enforcing the cyber law even after Indian IT Act 2000 got amended is still prevailing and is a great threat to our nation as whole and economy in particular. Since this paper is not focused on economical impacts, enforcement and how it can be effectively done I will be going less deeper on those aspects. But in some case studies you will definitely find how it was effectively imposed. I have also included a section on Cyber crime conviction and judgements in the end of this documents which covers some specific case studies on judgments.

The astonishing fact is that security as a service is estimated as $5.71 Billion in 2008 and is estimated to grow to US$ 16.98 Billion by year 2013 as quoted by an industry leading research firm IDC[2](http://satheeshgnair.blogspot.com/#FOOTNOTE-2).  Which means it may not be foolish for us to say that "if a venture capitalist invests in cyber crime he will make more money than he would do in any other technology business".

These facts may make your ears sharper, more so when you hear about increase in cyber criminality. Approximately 70 % of the threats on Internet are done by organised cyber criminals. 80 % of the 50 principal malicious codes could be used to reach confidential information. And as we wake up every day new vulnerabilities appear, each one having its own environment and its own consequences.

As per estimates only about 200 thousand people in the entire planet may be well qualified and certified to act against Hacking, Identity threat and Vulnerability or Cyber Criminality in general. This estimate is even far below compared to the required 2.1 Million experts required by the Information Security Industry itself as per an earlier study conducted by (ISC)2 International Information Systems Security Certification Consortium along with IDC[3](http://satheeshgnair.blogspot.com/#FOOTNOTE-3).

Now if you think your computer system is not being hacked and why the entire world is talking about hacking and making a big noise about this. May be you think this is a mere marketing technique by security vendors. The fact is that these professional intelligent criminals know where the money lies and if they have not hacked your system it is merely because they know there is nothing in it.

If you really want to experience the experience of being "hacked" start doing activities like net banking, money transfer, buy air tickets or start stock trading in your system without proper protection and antivirus software. Within weeks you can see the changes in your machine. You might think you have loaded extra applications to your system or the hard drive has become full. You might then download some anti-viruses and registry tweak with the help of of your computer support engineer. But even after he does everything and leaves your computer to yourself you will still feel your are driving a re-painted dented car, which just met with a fatal accident. The reason is very simple the bad guys have e-mapped your system and there is nothing that they have left unnoticed including the serial number of your hard drive to the mac address of your network card, well you may be now thinking that you are reading a horror movie story and if I have scared you that is what they do.

Some of you might have heard about 'Titan Rain'. If you have not it is the new type of world wide rampant hacking methodology. These are not about one poor hacker sitting in one secret basement and doing some malicious activity and doing it for a meal, just for fun or revenge sake. Titan Rain attacks are so flawless that they gain control of your system and compromise it and within 20 minutes after stealing everything of value and erase their entire tracks by the end, leaving no traces. This might again sound like science fiction where the aliens are trying to take control of the universe by attacking the central computer systems and some heroes are trying to protect the universe. But here these are anti-heroes and they are not trying to protect the universe and they are also with the aliens.

While talks about these types of hacking is going on, one distinction is that they are focused on sensitive information pertaining to government, military and supported relevant technologies.

While you may think, "What if they access some business data? How can it be a threat to our country?" I want to clarify here that they look for companies that supply food to the military, oil companies which makes special fuels to the government defense equipments and companies which has personal information about defense employees. The data collected is then traded to terrorist operations to exploit undercover military and government operations.

This is a real issue as you may see oil companies know where potentially valuable oil reserves might be. Telecommunications companies will have details about satellite communications and new technologies for improving communications reliability and bandwidth. Any organization with intellectual property worth protecting is a potential victim of these attackers and that is why they don't hack our home computers.

**Taxonomy**

Let's now spend some time understanding the various methods that are frequently used by criminals before we get on to the detailed discussions of Cyber crime examples. Most of this terms can be interpreted in different ways when it comes to practical usage and by the media. And my intention for putting this as a table here is to create a clear path for all categories of readers by familiarizing the terms so that their understanding gets enhanced.

|  |  |
| --- | --- |
| **Crimes focusing networks and hardware** | **Theft Of Services** |
| **Computer Intrusions** |
| **Computer Viruses, Worms, Trojan Horses, Spy-ware and Other Mal-ware** |
| **Distributed Denial of Service Attacks** |
| **Fraud and Deceptive Crimes** | **Internet Auction Fraud** |
| **Pay-Per Click Fraud** |
| **Nigerian Advance Fee Fraud** |
| **Reshipping Fraud** |
| **High Yield Investment Programs** |
| **Diploma Scam** |
| **Free Product and Service offers** |
| **Bogus Diet Patches** |
| **Phishing, Carding, and Money Laundering** |
| **Pumping and Dump Stock Fraud** |
| **Online Crimes** | **Spam** |
| **Scheduled Controlled Substances Sold Online without prescription** |
| **Child Exploitation/ Child Pornography and illegal Obscenity** |
| **Warez** |
| **Online Sale of Replica Counterfeit Trademarked Product** |
| **Untaxed Cigarettes Sold over the Internet** |
| **Online Gambling** |

**Theft Of Services**

Theft of services is, in many ways, the first "cyber" or "network-oriented" crime (albeit one which was originally committed against a phone network or a cable TV network rather than a modern packet-switched computer network). Phone phreaking involved things such as toll fraud, the "creative routing" of calls in non-optimal ways (e.g., call next door, but do so over long distance circuits nailed up literally around the world), and other things that folks weren't supposed to be doing. Cable TV theft of service typically involved unauthorized reception of basic or premium channel traffic, or the interception of microwave TV signals, w/o payment to the TV company. Some of these crimes, or their Internet analogs, continue today, although the world is a vastly different place today, and most theft-of-service crimes have evolved over the years.[4](http://satheeshgnair.blogspot.com/#FOOTNOTE-4)

**Computer Intrusions**

There are various definitions you an find about computer intrusion and let me tell you there is no one "real" definition available. Following are some excerpts form the federal rules.

Any person commits computer crime who knowingly accesses, attempts to access or uses, or attempts to use, any computer, computer system, computer network or any part thereof for the purpose of:

* Devising or executing any scheme or artifice to defraud;
* Obtaining money, property or services by means of false or fraudulent pretenses, representations or promises; or
* Committing theft, including, but not limited to, theft of proprietary information.

Any person who knowingly and without authorization uses, accesses or attempts to access any computer, computer system, computer network, or any computer software, program, documentation or data contained in such computer, computer system or computer network, commits computer crime.

**Computer Viruses, Worms, Trojan Horses, Spy-ware and Other Mal-ware**

Mal-ware is software designed to infiltrate or damage a computer system without the owner's informed consent. It is a portmanteau of the words "malicious" and "[software](http://www.newworldencyclopedia.org/entry/Computer_software)." The expression is a general term used by computer professionals to mean a variety of forms of hostile, intrusive, or annoying software or program code. The more specific term "computer virus" is however used in common parlance, and often in the [media](http://www.newworldencyclopedia.org/entry/Mass_media), to describe all kinds of Mal-ware.

Software is considered mal-ware based on the perceived intent of the creator rather than any particular features. It includes computer viruses, worms, Trojan horses, spy-ware, dishonest ad-ware, and other malicious and unwanted software. In law, mal-ware may also be referred to as a "computer contaminant."[[2]](http://www.newworldencyclopedia.org/entry/Cybercrime#cite_note-1)

Many early infectious programs, including the Internet worm and a number of MS-DOS viruses, were written as experiments or pranks generally intended to be harmless or merely annoying rather than to cause serious damage. Since the rise of widespread broadband [Internet](http://www.newworldencyclopedia.org/entry/Internet) access, more malicious software has been designed for a profit motive. For instance, since 2003, the majority of widespread viruses and worms have been designed to take control of users' computers for [black market](http://www.newworldencyclopedia.org/entry/Black_market) exploitation. Infected "zombie computers" are used to send [e-mail spam](http://www.newworldencyclopedia.org/entry/Cybercrime#Spam), to host contraband data such as [child pornography](http://www.newworldencyclopedia.org/entry/Cybercrime#Child_Pornography), or to engage in [distributed denial-of-service](http://www.newworldencyclopedia.org/entry/Cybercrime#Denial_of_service_attacks) attacks as a form of [extortion](http://www.newworldencyclopedia.org/entry/Extortion).[[3]](http://www.newworldencyclopedia.org/entry/Cybercrime#cite_note-2)

Another strictly for-profit category of mal-ware has emerged in spy-ware—programs designed to monitor users' web browsing, display unsolicited [advertisements](http://www.newworldencyclopedia.org/entry/Advertising), or redirect affiliate marketing revenues to the spy-ware creator. Spy-ware programs do not spread like viruses; they are generally installed by exploiting security holes or are packaged with user-installed software.[5](http://satheeshgnair.blogspot.com/#FOOTNOTE-5)

**Distributed Denial of Service Attacks**

A denial-of-service attack or Distributed Denial or Service (DoS attack) is an attempt to make a computer resource unavailable to its intended users. Although the means to, motives for, and targets of a DoS attack may vary, it generally comprises the concerted, malevolent efforts of a person or persons to prevent an [Internet](http://www.newworldencyclopedia.org/entry/Internet) [site](http://www.newworldencyclopedia.org/entry/Website) or service from functioning efficiently or at all, temporarily or indefinitely. Perpetrators of DoS attacks typically—but not exclusively—target sites or services hosted on high-profile web servers. Denial of service attacks are one form of computer [sabotage](http://www.newworldencyclopedia.org/entry/Sabotage) whereby people can effectively ruin their target's operations for what could be a lengthy period of time.[6](http://satheeshgnair.blogspot.com/#FOOTNOTE-6)

**Internet Auction Fraud**

Online auctions have transpired into a very lucrative business. Many are making a living at buying/selling through online auction houses. Millions of online auction items are up for bid daily and include items from all around the world. This phenomenon keeps growing daily as more buyers and sellers flock to these online auction houses. This activity is offering great opportunities for buyers and sellers. Sellers are able to have their posted item viewed by millions of people and buyers are able to purchase hard to find items and/or items at discounted prices. However, these online auctions are also giving perpetrators another avenue to perpetrate fraud.

Internet auction fraud is currently the number one fraud committed over the Internet. The Internet Fraud Complaint Center (IFCC) lists auction fraud entailing 64% of more than 30,000 complaints received.[7](http://satheeshgnair.blogspot.com/#FOOTNOTE-7)

**Pay-Per Click Fraud**

Click fraud (sometimes called *pay-per-click fraud*) is the practice of artificially inflating traffic statistics to defraud advertisers or Web sites that provide venues for advertisers. In the common pay-per-click advertising model, advertisers pay a fee for each click on their link. According to a CNET News article some industry segments have costs-per-click of several dollars. By using automated clicking programs (called hit bots) or employing low-cost workers to click the links, the perpetrators create the illusion that a large number of potential customers are clicking the advertiser's links, when in fact there is no likelihood that any of the clicks will lead to profit for the advertiser.

Click fraud scammers often take advantage of the affiliate programs offered by some Web sites, such as Google and Yahoo! Search Marketing. The scammers sign up for the affiliate programs, agreeing to provide further exposure to the advertising in question and receiving a portion of the pay-per-click fees in return. The perpetrators place the ads on Web sites created solely for this purpose that, naturally, don't have any real traffic. Once the ads are in place, the hitbots or workers generate large volumes of fraudulent clicks, often in a very short time period, for which the scammer bills the owner of the affiliate program. Both Google and Yahoo! Search Marketing have had to reimburse advertisers for pay-per-click fees that were discovered to have been the result of click fraud.[8](http://satheeshgnair.blogspot.com/#FOOTNOTE-8)

**Nigerian Advance Fee Fraud**

Nick named as the 419 fraud  it is very familiar fraud to most us who are avid Internet users. Here the fraudster starts his operations with a letter something like below.  It is estimated that more than 15 business men have been been kidnapped and killed as a part of AFF scam in Nigeria. In fact I have received a similar mail even on 23rd June 2009.

From: "Mr. Don Peter" To: undisclosed-recipients:;  
  
Subject: Dear Friend  
  
Date: Thu, 18 Oct 2007 08:39:10 -0400  
  
Reply-to: hellen\_doris1@yahoo.fr  
  
  
  
Dear Friend

It has been long we communicate last, am so sorry for the delay, I want to Inform you that your cheque of ($850.000.00) Which my boss asked me to mail to you as soon as you requested it, is still with me.

But due to some minute issue you fails to respond at the Appropriate time, and presently the cheque is with me here in LAGOS-NIGERIA Though i had a new contact from a friend of mine who works with one security company here in NIGERIA that will deliver you your cheque at your door step with a cheaper rate, which the company said that it will cost you the sum of $198.00 usd, So you have to Contact them and register with them now.

After a victim responds positively to an AFF letter by sending the required documentation (for example, signed company letterheads, bank account number, etc.) the hook is in. The  primary reason for the documentation is not to rob the victim’s bank account, but to perpetuate the illusion that the deal is legitimate and moving forward. The blank signed letterheads are altered and used by the criminals as props in other frauds, letters of reference to obtain visas, or sold to other AFF criminals.

For the next week to 10 days, the perpetrators establish a level of trust with the victim. This is accomplished by sending the victim more “official” documentation verifying the bonafides of the deal and the people involved. The criminals will correspond with the victim via fax machines and courier mail because it is difficult to trace. In the past, these criminals made extensive use of business centers in Lagos to place phone calls and send faxes, but the Nigerian Government reports—and evidence seems to confirm—that business centers were closed in an effort to thwart AFF scams.[9](http://satheeshgnair.blogspot.com/#FOOTNOTE-9)

**Reshipping Fraud**

This scam is everywhere. Some advertisements are placed in newspapers, and you can even find listings on CareerBuilder.com as well as other job placement websites. When you answer the ad, the reshipping "employer" will ask that you send your personal information such as your social security number and date of birth. After the employer receives your information, packages will start arriving at your house with instructions on how to repackage and then ship the goods to addresses abroad.  
  
  
  
When your payment for services performed arrives, it will be in the form of a third party cashier's check. This should raise red flags on your part since the accepted way of doing business is with a paycheck. These cashier's checks will usually be greater than the initially agreed amount. Then the employer will ask that you send back electronically what was overpaid to you. The moment you have completed this transaction, another problem arises. The bank will discover that the cashier's check was fake and hold you responsible for the full amount of the check. In addition, your "employer" has your personal information which will be used to defraud more unsuspecting people who become "employees" of this illegal money making scheme. You, the re-shipper, can get into big trouble because all the goods that you shipped overseas was bought with stolen credit cards. [10](http://satheeshgnair.blogspot.com/#FOOTNOTE-10)

**High Yield investment programs**

HYIP stands for High Yield Investment Program. They are the sites out there that promise you a 1% daily return on your money or some such nonsense. Most of them claim that they are brilliant with stocks or futures or foreign currencies and all you need to do is send your money to them and they will pay you back at the rate of 1% a day or double your money in 3 months or something along those lines.

HYIP’s are not investments and while they may be high yield for some people for a short time eventually they become zero yield when your money disappears.

There is no way to know how much money is taken from people every day through these types of programs, but judging by the number of them and how quickly they spring up and go away I wouldn’t be surprised no matter how high the number is. The reason they spring up so quickly is that you can actually purchase programs that run a HYIP on your website. Or you can simply buy a website that’s already been set up as a HYIP and is ready to start taking money. Programmers can put these together from templates very quickly. Once the website is up and running it is so simple to put any kind of information on there you wish. If you’re planning on stealing people’s money do you care if it’s the truth? Of course you don’t, you’re just like any other con man and you’re gonna tell your victim whatever you need to so you can part them from their money.

So you tell the world that you are one of the top stock brokers or commodity brokers or FOREX traders and you have a “NEW” system that will put money in their pockets even while they sleep. Will people believe you? Yep, some will because now you have the attention of their greed. Of course you want it to look like your program is already successful because that will make your lies even more believable. So, when you set up the website you also put counters on there with large numbers to show how many people are already making money with you. Yes it’s another lie, but what do you care you’re getting rich. Now you have even more people buying into the program, but you can make it look even better. What if you had testimonials from ‘real’ people who made money with your program. Easy! Set up a forum and pay some people to put a few dozen posts in there about how wonderful your HYIP is and how rich they’re becoming. The costs for the forum posts is minimal compared to the amount of money that will soon be flowing your way. Now with everything in place you start advertising your new HYIP. In the beginning everything is going to look great to your “investors” because you’ll pay out to everyone on time. And you’ll set up an affiliate program as well for others to promote your great HYIP. And you’ll pay them on time as well. If you do this then you’ll be able to get hundreds of new “investors” in just a short period of time. Your “investors” will be ecstatic as they receive their payments and as greed takes over they will “re-invest”, send every penny right back to you to make as much money as possible. Eventually the owners of the HYIP will have several hundred thousand dollars and that’s when they pull the plug and POOF!…they disappear.

There are thousands of documented cases of HYIP fraud. Some people have even lost their life’s savings this way, please don’t be one of those people.[11](http://satheeshgnair.blogspot.com/#FOOTNOTE-11)

**Diploma Scam**

Quick degree scams - "Get your degree in 30 days!" "No studying required", "Turn your experience into a degree". They say they are accredited and the degree is legal and meaningful. That's part of the scam.

The existence of unaccredited, substandard, and/or fraudulent postsecondary education (college, university, graduate schools) providers is a global phenomenon, as is the existence of unrecognized and/or fraudulent accreditors. The credits and degrees awarded by these unaccredited or sham diploma mills are not going to be recognized by legitimately accredited institutions, official professional licensing authorities, recognition authorities or reputable employers.

And when the scam is exposed that you purchased your degree; you'll be out on the street and no one will hire you.  You may make the cover of a newspaper, exposed as the worthless hack you are for attempting to buy your degree. You may make a list of people who have purchased scam degrees, that we're working on right now.[12](http://satheeshgnair.blogspot.com/#FOOTNOTE-12)

**Free Product and Service offers**

Free stuff is being used as a marketing or brand awareness tool, but it can be used for a much more sinister goal: It can be the tool to collect a significant amount of money via simple social engineering.

I get offers for many products by e-mail which i mostly delete or let the spam filter take care of them. But in the past week i got bombarded from several different sources regarding one apparently free product. The sheer amount of e-mails made me read through one of them. It was an announcement for a free distribution of some SEO program.

Just for fun, I clicked on the included link, and got to a page with a style of a typical social engineering 'easy money' page. Here is the analysis of such pages.

At the end of the (very long) page i got to the real deal. They need my credit card in order to send me the free program on a DVD

* I will be charged just shipping and handling costs for the program which are $7 for US and $10 internationally, and i get free access to the service for a month.
* I will be billed $100 per month for the SERVICE, after the first month. I understand that I can cancel at any time right from within the site or by just logging a ticket at www.SOMEADDRESS.TLD

Wait, if it is a FREE PROGRAM delivered on a DVD with no strings attached, they can just dump it on rapid-share and let the visitors rip.

The fraudsters model is simple they always have access to thousands of credit card data with an agreement to use them when they want.

**Bogus Diet Patches**

Another common method were criminals try to woo people by offering highly discounted patches. In reality what gets shipped would be only a dummy patch or a fake drug. The shipping is done normally using re-shipping method.[13](http://satheeshgnair.blogspot.com/#FOOTNOTE-13)

**Phishing, Carding, and Money Laundering**

"Phishing is a form of online identity theft that employs both **social engineering** and **technical subterfuge** to steal consumers' personal identity data and financial account credentials. Social-engineering schemes use 'spoofed' e- mails to lead consumers to counterfeit websites designed to trick recipients into divulging financial data such as account user names and passwords. Hijacking brand names of banks, e-retailers and credit card companies, phishers often convince recipients to respond. **Technical subterfuge** schemes plant **crime-ware** onto PCs to steal credentials directly, often using key logging systems to intercept consumers online account user names and passwords, and to corrupt local and remote navigational infrastructures to misdirect consumers to counterfeit websites and to authentic websites through phisher-controlled proxies that can be used to monitor and intercept consumers’ keystrokes."

**Pumping and Dump Stock Fraud**

"Pump and dump" schemes, also known as "hype and dump manipulation," involve the touting of a company's stock (typically microcap companies) through false and misleading statements to the marketplace. After pumping the stock, fraudsters make huge profits by selling their cheap stock into the market.

Pump and dump schemes often occur on the Internet where it is common to see messages posted that urge readers to buy a stock quickly or to sell before the price goes down, or a telemarketer will call using the same sort of pitch. Often the promoters will claim to have "inside" information about an impending development or to use an "infallible" combination of economic and stock market data to pick stocks. In reality, they may be company insiders or paid promoters who stand to gain by selling their shares after the stock price is "pumped" up by the buying frenzy they create. Once these fraudsters "dump" their shares and stop hyping the stock, the price typically falls, and investors lose their money.

**Spam**

You've seen spam (unsolicited commercial email) show up as a component of some cyber crimes we've already discussed, but I think that ultimately it also deserves its own listing here, because at least in some cases bulk mail may be legal or illegal based solely on what's being sent and how it is being delivered. In some jurisdictions, any or all commercial email is permissible, but in other jurisdictions,  unsolicited commercial email is regulated.

**Scheduled Controlled Substances Sold Online without prescription**

There are many scheduled controlled substances sold online. All you need in one credit card to buy them. You don't need a prescription, social security number or age proof to buy them. For example.

* In the United States, the Controlled Substances Act (CSA) regulates the manufacture and distribution of narcotics, stimulants, depressants, hallucinogens, anabolic steroids, and chemicals used in the illicit production of controlled substances. See 21 USC 811.
* Substances are categorized by the CSA into five tiers, I through V:  
    
  -- Schedule I: heroin, LSD, marijuana, MDMA, peyote, psilocybin, etc.  
    
  -- Schedule II: cocaine, methamphetamine, methylphenidate, morphine, PCP, etc.  
    
  -- Schedule III: anabolic steroids, codeine/acetaminophen combinations, etc.  
    
  -- Schedule IV: alprazolam, diazepam, phentermine, zolpidem, etc.  
    
  -- Schedule V: codeine-based cough syrups, etc.  
    
  See the summary table at http://www.usdoj.gov/dea/pubs/scheduling.html
* States can also schedule controlled substances beyond federal levels; for example, while carisoprodol ("Soma") is not a federally controlled substance at the time this was written, it **IS** scheduled by Oregon and other individual states (see http://www.deadiversion.usdoj.gov/drugs\_concern/carisoprodol.htm )
* Other drugs (such as antibiotics, insulin, birth control pills, ED pills) require a bona fide prescription, but they're regulated by the FDA rather than the DEA.
* Fraudsters contact their victims by bulk email and conduct a fraud transaction

**Child Exploitation/ Child Pornography and illegal Obscenity**

I request if you ever come across a child pornographic site please report. Please do not do the research yourself.

* Internet porn is a multi-billion dollar-per-year industry with content ranging from the risque to the hardcore; thus, it is hardly surprising that there is a variety of content-related cyber crimes associated with this online content area.
* Perhaps more than any other online crime related area, child porn is one area where any and **all** investigation of potentially illegal content **MUST** be left to law enforcement. If you run into a child porn site do **NOT** attempt to investigate it yourself! Instead, report it immediately to the NCMEC or the FBI's Innocent Images program (see http://www.fbi.gov/innocent.htm )

**Warez**

* "Warez" (pronounced "wearzz," NOT "wahr-ez") are pirated copies of proprietary commercial software, typically distributed over the Internet after the program's copyright protection mechanisms (if any) have been disabled. Pirated music, pirated movies and pirated games may also be distributed.
* Individuals in the warez scene may amass and freely share huge collections of programs (even if they have no personal use for particular programs) as a competitive matter or to increase their status with their peers; others may avoid an emphasis on sheer volume, focusing instead on how quickly they can get and distribute newly developed programs or particularly obscure or expensive ones.
* Others may accumulate titles to build an inventory of programs which can be sold to retail customers online. These pirates typically attempt to explain their unusually low prices (and unorthodox distribution mechanisms) by falsely claiming that the downloadable software they're selling is an "original equipment manufacturer" ("OEM") version which is inexpensive because it is being distributed without physical media, manuals or or fancy packaging.   
    
  In reality, of course, that software is sold cheaply because it's been stolen.
* Stolen intellectual property may also be distributed in the form of authentic- looking physical CD or DVD copies, again typically sold at large discounts.

**Online Sale of Replica Counterfeit Trademarked Product**

Counterfieting is a very old industry it is as old as the brand. Coupled with Online presence it has shot into a completely new business today. The counterfeiting industry costs $300 billion in the US annually, $500 billion worldwide.

In case you aren't aware of this, MANY (estimated to be over 50%) of the "100% guaranteed authentic" designer & big name brand items you see on auction sites are fake.[14](http://satheeshgnair.blogspot.com/#FOOTNOTE-14)

**Untaxed Cigarettes Sold over the Internet**

Online cigarette sale is big tax evading game in the west.&nbsp;Internet cigarette sellers offer cheaper rates in part because they do not collect state taxes. Under legal pressure, they began turning over customer data to states a year ago. A federal law prohibits retailers from delivering tobacco products across state lines without reporting their sales.[15](http://satheeshgnair.blogspot.com/#FOOTNOTE-15)

**Online Gambling**

Online gambling has become the number one Internet-related card fraud problem in Europe. That's according to Europay, Mastercard's European partner, which reckons that 20 per cent of online fraud is related to gambling. Online fraud accounts for five per cent of all UK credit and debit card fraud[16](http://satheeshgnair.blogspot.com/#FOOTNOTE-16).

Internet gambling, like Internet porn, is big business – a USA Today article puts its value at $12 billion dollars per year.[17](http://satheeshgnair.blogspot.com/#FOOTNOTE-17) Calvin Ayre (of the Bodog Internet gambling empire) even made Forbes list of billionaires[18](http://satheeshgnair.blogspot.com/#FOOTNOTE-18). While Internet gambling is legal in some jurisdictions, in the United States, with only narrow exceptions, Internet gambling is NOT legal

**Cyber Crime in India: Case Studies**

While I have a huge collection of international cyber crimes I thought it may be more relevant if we discuss Indian Cyber crime case studies. However if any of you is interested in international case studies please do reach me. I have not arranged the following section in an order to create flow of thought for the reader. And it is possible there is a drift from the taxonomy which we have defined in the beginning.

**Insulting Images of Warrior Shivaji on Google - Orkut**[**19**](http://satheeshgnair.blogspot.com/#FOOTNOTE-19)

An Indian posts ‘insulting images’ of respected warrior-saint Shivaji on Google’s Orkut.  Indian police come knocking at Google’s gilded door demanding the IP address (IP uniquely identifies every computer in the world) which is the source of this negative image.  Google, India hands over the IP address.

No such incident in India would be complete without a few administrative slip-ups.  The computer with that IP address is using Airtel, India as the ISP to connect to the internet and Orkut.  Airtel gives police the name of an innocent person using a different IP address.  How two IP addresses could be mixed-up in a sensitive police case is anyone’s guess.

An innocent Indian, Lakshmana Kailash K, is arrested in Bangalore and thrown in jail for 3 weeks.  Eventually, his innocence is proved and he is released in Oct, 2007.

A number of  news media report this incident.  American citizen and India lover Christopher Soghoian (home page http://www.dubfire.net/chris/) studies Informatics at Indiana University and researches/writes about security, privacy and computer crime.  Christopher does an excellent article on this topic for the blogs at respected tech media group CNET.

Like all good writers, Christopher Soghoian, gives Google, India a list of questions so that he can give a balanced perspective to the millions of CNET readers.

**How does Google, India respond?**

The only comment was:  "Google has very high standards for user privacy and a clear privacy policy, and authorities are required to follow legal process to get information. In compliance with Indian legal process, we provided Indian law enforcement authorities with IP address information of an Orkut user."

Not surprisingly, Google is a keen to play this down as Yahoo is being hauled over the coals by US Congress for handing over an IP addresses and emails to the Chinese Government which resulted in a Chinese democracy activist being jailed.

Techgoss contacted Christopher and asked him for a list of  the questions he had put to Google. The following were the questions that Christopher put to Google which were never answered.  Sometimes what you do not say says more about what you have done.

1. Can Google speak at all to the specifics of this incident?

2. If so, can Google confirm if they released ip addresses or any other log information to the Indian police regarding this incident.

3. If Google did hand over log information, did the Indian police have a warrant/court order, or did they merely request it?

4. Does Google feel in any way responsible for the man's accidental arrest and jailing?

5. Speaking more generally, without going into the specifics of this incident...Has Google ever in the past handed over user information (including logs) to Indian law enforcement/authorities without a court order/search warrant?

6. In this case, the crime the man was accused of (defaming a 300 year old historical figure)  does not exist in the US. Will Google conform to the laws of each country it does business in, or will it defer to American concepts of freedom of speech and the press?

7. Does Google reveal information to other countries for "crimes" that would not normally be an illegal in the US? For example, the ip addresses of people in Saudi Arabia and other conservative Muslim countries who search for adult, consensual pornography?

8. Is the log data for Orkut stored in India, or is it stored elsewhere? If the data is not stored in India, is Google still responsible for giving it to the Indian authorities?

**How does it Airtel react to rectify its mistake?**

Firstly, with an immediate, unqualified apology.   In itself, a positive first step.

Techgoss (techgoss.com)  had heard rumors about Airtel also offering monetary compensation to the person wrongly jailed.   But Airtel is being coy about possible financial compensation.  An Airtel spokesperson issued the following statement to techgoss.com

“Airtel are aware of this incident and deeply distressed by the severe inconvenience caused to the customer. We are fully cooperating with the authorities to provide all information in this regard and we are in touch with the customer. We have robust internal processes, which we review frequently to make them more stringent. We have conducted a thorough investigation of the matter and will take appropriate action”.

Does this mean the customer will get compensation?  It is not clear either way.  Let’s wait and see.  It is interesting to see that despite the arrest he is still with Airtel.  Now that’s loyalty to your telecom company.

**What is the current Scenario?**

Finally he has demanded that he be compensated for the injustice meted out to him! The illegally accused and detained techie in the Chatrapati Shivaji defamation picture case on Orkut, Lakshmana Kailas K, has slapped a ten page legal notice on Telecom giant Bharti Airtel, the Principal Secretary (Home) of the state government in Maharashtra, India and the Assistant Commissioner of Police (Financial & Cyber crime unit) demanding that an amount of 20 crores be paid as damages.

The software engineer has also sent a copy of the legal notice to the National Human rights commission. Lakshmana had spent a harrowing 50 days in police custody accused of a crime he had never committed just because an IP address sought by the police was wrongly supplied by Bharti Airtel. The legal notice smacks of his anger with the police and judiciary making a mockery of the rights of an individual and the pitiable conditions of the Yerwada jail where he was detained with a number of hardened criminals. He is reported to have been beaten by a lathi and asked to use the same bowl to eat and to use in the toilet.

**Kenneth L. Haywood**

Kenneth L. Haywood  (born 1964) became involved in a 2008 controversy in the Indian city of Mumbai after his wireless connection was allegedly used by terrorists to transmit a message to Indian news networks before their attacks. It was subsequently revealed that Haywood had been living a double life as an "executive skills trainer" and a Christian pastor, while the firm that he worked for was a probable front for evangelical religious activities. Haywood was not charged by Indian authorities in connection with the blasts, which occurred at [Ahmedabad](http://en.wikipedia.org/wiki/2008_Ahmedabad_bombings) and Surat, in late July 2008.

**Financial crimes**[**20**](http://satheeshgnair.blogspot.com/#FOOTNOTE-20)

[Wipro Spectramind](http://www.indiaforensic.com/wipro.htm) lost the telemarketing contract from Capital one due to an organized crime.The telemarketing executives offered fake discounts, free gifts to the Americans in order to boost the sales of the Capital one. The internal audit revealed the fact and surprisingly it was also noted that the superiors of these telemarketers were also involved in the whole scenario.

**Cyber pornography**

Some more Indian incidents revolving around cyber pornography include the Air Force Balbharati School case. In the first case of this kind, the Delhi Police Cyber Crime Cell registered a case under section 67 of the IT act, 2000. A student of the Air Force Balbharati School, New Delhi, was teased by all his classmates for having a pockmarked face.

**[Online gambling](http://www.indiaforensic.com/cyberlotto.htm)**

Recent Indian case about cyber lotto was very interesting. A man called Kola Mohan invented the story of winning the Euro Lottery. He himself created a website and an email address on the Internet with the address 'eurolottery@usa.net.' Whenever accessed, the site would name him as the beneficiary of the 12.5 million pound.After confirmation a telgu newspaper published this as a news. He collected huge sums from the public as well as from some banks for mobilization of the deposits in foreign currency. However, the fraud came to light when a cheque discounted by him with the Andhra Bank for Rs 1.73 million bounced. Mohan had pledged with Andhra Bank the copy of a bond certificate purportedly issued by Midland Bank, Sheffields, London stating that a term deposit of 12.5 million was held in his name.

**Intellectual Property crimes**

These include software piracy, copyright infringement, trademarks violations, theft of computer source code etc. In other words this is also referred to as cybersquatting. Satyam Vs. Siffy is the most widely known case. Bharti Cellular Ltd. filed a case in the Delhi High Court that some cyber squatters had registered domain names such as barticellular.com and bhartimobile.com with Network solutions under different fictitious names. The court directed Network Solutions not to transfer the domain names in question to any third party and the matter is sub-judice. Similar issues had risen before various High Courts earlier. Yahoo had sued one Akash Arora for use of the domain name ‘Yahooindia.Com’ deceptively similar to its ‘Yahoo.com’. As this case was governed by the Trade Marks Act, 1958, the additional defence taken against Yahoo’s legal action for the interim order was that the Trade Marks Act was applicable only to goods.

**[Email spoofing](http://www.indiaforensic.com/cyberextrotion.htm)**

Recently, a branch of the Global Trust Bank experienced a run on the bank. Numerous customers decided to withdraw all their money and close their accounts. It was revealed that someone had sent out spoofed emails to many of the bank’s customers stating that the bank was in very bad shape financially and could close operations at any time. Unfortunately this information proved to be true in the next few days.

But the best example of the email spoofing can be given by the Gujarat Ambuja Executive’s case. Where he pretended to be a girl and cheated the Abu dhabi based NRI for crores by blackmailing tactics.

**Cyber Defamation**

India’s first case of cyber defamation was reported when a company’s employee started sending derogatory, defamatory and obscene e-mails about its Managing Director. The e-mails were anonymous and frequent, and were sent to many of their business associates to tarnish the image and goodwill of the company.

The company was able to identify the employee with the help of a private computer expert and moved the Delhi High Court. The court granted an ad-interim injunction and restrained the employee from sending, publishing and transmitting e-mails, which are defamatory or derogatory to the plaintiffs.

**Cyber stalking**

Ritu Kohli has the dubious distinction of being the first lady to register the cyber stalking case. A friend of her husband gave her telephonic number in the general chat room. The general chatting facility is provided by some websites like MIRC and ICQ. Where person can easily chat without disclosing his true identity. The friend of husband also encouraged this chatters to speak in slang language to Ms. Kohli.

**Unauthorized access to computer systems or networks**

However, as per Indian law, unauthorized access does occur, if hacking has taken place. An active hackers’ group, led by one “Dr. Nuker”, who claims to be the founder of Pakistan Hackerz Club, reportedly hacked the websites of the Indian Parliament, Ahmedabad Telephone Exchange, Engineering Export Promotion Council, and United Nations (India).

**IPR Theft**

Jun 23, 2009 at 0119 hrs IST

The economic offences wing (EOW) of the Pune police on Monday arrested a software engineer Asma Sandip Thorve (37), a resident of Uday Society in Sahkar Nagar, for allegedly cheating Brainvisa Technologies to the tune of Rs 46.5 crores, by stealing their source code. Earlier, the police had arrested software engineer Sameer Ashok Inamdar (36) of Kondhwa in the same case.

According to the police, Inamdar resigned from Brainvisa Technologies in August 2006. He allegedly stole the source code and other secret information of Brainvisa Technologies and started his own company. Owner of Brainvisa Technologies Nitin Hemchandra Agarwal had lodged a police complaint alleging that the company lost Rs 46.5 crores due to this.

A team, led by assistant commissioner Pushpa Deshmukh, arrested Thorve, who was Inamdar’s business partner and allegedly provided him the confidential data of Brainvisa.

Thorve worked as senior manager, business development, for Brainvisa from May 2004 to December 2005 and there on as vice president till December 2008, after which she joined Inamdar as a partner. Thorve was produced before court on Monday and has been remanded to police custody till June 26.

**Email bombing (DoS)**

In one case, a foreigner who had been residing in Simla, India for almost thirty years wanted to avail of a scheme introduced by the Simla Housing Board to buy land at lower rates. When he made an application it was rejected on the grounds that the scheme was available only for citizens of India. He decided to take his revenge. Consequently he sent thousands of mails to the Simla Housing Board and repeatedly kept sending e-mails till their servers crashed.

**Data diddling**

The NDMC Electricity Billing Fraud Case that took place in 1996 is a typical example. The computer network was used for receipt and accounting of electricity bills by the NDMC, Delhi. Collection of money, computerized accounting, record maintenance and remittance in he bank were exclusively left to a private contractor who was a computer professional. He misappropriated huge amount of funds by manipulating data files to show less receipt and bank remittance.

**Internet time theft**

This connotes the usage by an unauthorized person of the Internet hours paid for by another person. In May 2000, the economic offences wing, IPR section crime branch of Delhi police registered its first case involving theft of Internet hours. In this case, the accused, Mukesh Gupta an engineer with Nicom System (p) Ltd. was sent to the residence of the complainant to activate his Internet connection. However, the accused used Col. Bajwa’s login name and password from various places causing wrongful loss of 100 hours to Col. Bajwa. Delhi police arrested the accused for theft of Internet time.

On further inquiry in the case, it was found that Krishan Kumar, son of an ex army officer, working as senior executive in M/s Highpoint Tours & Travels had used Col Bajwa’s login and passwords as many as 207 times from his residence and twice from his office. He confessed that Shashi Nagpal, from whom he had purchased a computer, gave the login and password to him. The police could not believe that time could be stolen. They were not aware of the concept of time-theft at all. Colonel Bajwa’s report was rejected. He decided to approach The Times of India, New Delhi. They, in turn carried a report about the inadequacy of the New Delhi Police in handling cyber crimes. The Commissioner of Police, Delhi then took the case into his own hands and the police under his directions raided and arrested Krishan Kumar under sections 379, 411, 34 of IPC and section 25 of the Indian Telegraph Act. In another case, the Economic Offences Wing of Delhi Police arrested a computer engineer who got hold of the password of an Internet user, accessed the computer and stole 107 hours of Internet time from the other person’s account. He was booked for the crime by a Delhi court during May 2000.

**SBI arm wins cybersquatting case - Peeyush Agnihotri - Tribune News Service**

Chandigarh, August 24  
  
SBI Card and Payment Services Private Limited, the credit card arm of the State Bank of India (SBI), received a shot in the arm when it won a case of cybersquatting against Domain Active Pty Limited, an Australian dotcom company.

The judgement, a notification of which was received earlier this week, was delivered by the administrative tribunal constituted by the World Intellectual Property Organisation (WIPO), Geneva.

Established in 1998, SBI Card and Payment Services Private Limited is a joint venture between GE Capital Services, the largest issuer of private label credit cards in the world, and the State Bank of India (SBI), the largest Indian bank. SBI holds 60 per cent stake while GE 40 per cent.

The venture offers a range of credit cards — SBI Classic Card, SBI Gold Card, SBI International Card, SBI Doctors Card. It also has a number of city affinity cards (SBI Kolkata Card, SBI Mumbai Card, SBI Delhi Card, SBI Hyderabad Card, SBI Bangalore Card), commanding sales of over one million.

It all began when Domain Active Pty Limited, an Australian entity, floated a website on the domain name, www.sbicards.com, and even ‘tricked’ financial big–time entities like Chase Manhattan into advertising on the site.

The SBI arm, which had already registered the domain name with Fabulous.Com Pty. Ltd, lodged a complaint on March 16 at the World Intellectual Property Organisation (WIPO), Geneva.

The WIPO Administrative Panel found that the Australian entity’s website could have attracted potential attention from the public because of its affiliation with SBI Cards’ products and services. At the same time it created a risk of confusion with the products/services and trademark as to the source, sponsorship, affiliation or endorsement of its website.

The panel’s independent verification showed that the current use of the Australian firm’s website, www.sbicards.com, was practically the same. The panel held that the respondent (Domain Active Pty Limited) “has registered the disputed domain name in bad faith”.

Talking exclusively to The Tribune from New Delhi, Mr Rodney D. Ryder, who represented SBI Cards, said that it was a clear case of cyber fraud and cybersquatting. “The judgement has come as big relief. No penalty could, however, be imposed on the errant firm since at WIPO we have not been able to evolve a consensus on what should be the proper damage/compensation amount as the cases involve the jurisdiction clause,” he said.

**Credit Card Frauds**

Amit Tiwari had many names, bank accounts and clients. None of them were for real. With a plan that was both ingenious and naïve, the 21-year-old engineering student from Pune tried to defraud a Mumbai-based credit card processing company, CC Avenue, of nearly Rs 900,000.He was arrested by the Mumbai Police on August 21, 2003 after nearly an year of hide and seek with CC Avenue. He's been charged for cheating under Section 420.

CC Avenue verifies and validates credit cards of buyers for over a thousand e-commerce Web sites. It conducts checks like IP mapping, zip code mapping and reverse lookup of telephone numbers.Amit Tiwari found a way to bypass them.In May 2002, Col Vikram Tiwari signed up for CC Avenue's services. In November, he requested the company to deal with his son, Amit, who offered Web designing services on www.mafiaz.com. CC Avenue's security team confirmed his credentials through bank signature verification, driving license and his HDFC Bank debit card. Everything was genuine.Amit processed several transactions, worth Rs 311,508, via CC Avenue from November 2002 to February 2003. Then the transactions stopped.In April 2003, CC Avenue began receiving charge-backs from the credit card holders, who denied using mafiaz.com's Web designing service.Amit had assumed the identities of these 'customers', and purchased mafiaz.com's services with credit card details that he found on the Net. He was both the buyer and the seller.Calls to Amit's house in Lucknow went unanswered. Legal notices came back unclaimed. Amit had disappeared without a trace.

**[Three-in-one fraudster](http://www.tribuneindia.com/2005/20050825/biz.htm" \l "top#top)**

In June 2003, Sachin Deshpande and Jeevan Palani signed separate agreements with CC Avenue to provide Web designing services through their sites www.infocreek.org and www.ewebsitestarter.com. The company's risk-management team found that both these sites had ripped off content and even the client list from foreign sites with similar names. The modus operandi was similar to Amit's. Vishwas Patel, the CEO of CC Avenue, spoke to Sachin over the phone and found that he sounded just like Amit - "young and immature". They decided to hold back payment.

Then, a person called Shoaib Sharif sought the services of CC Avenue. Vishwas and his team again spotted a similar pattern. They held back payment on various pretexts. "He sounded desperate," says Vishwas. So they decided to trap him.

**[Trapped](http://www.tribuneindia.com/2005/20050825/biz.htm" \l "top#top)**

CC Avenue's accounts manager asked Shoaib to come to Mumbai to collect a cheque of Rs 40,000. On August 21, a young man walked into Vishwas's office. He introduced himself as Shoaib Sharif. Vishwas immediately recognized him as Amit. (He had seen Amit's photograph from his driver's license). Vishwas then called the Mumbai Police, who rushed to his office and picked up the lad. At the Santa Cruz police station, the boy confessed right away.

**India's First ATM Card Fraud**

The Chennai City Police have busted an international gang involved in cyber crime, with the arrest of Deepak Prem Manwani (22), who was caught red-handed while breaking into an ATM in the city in June last, it is reliably learnt.  
  
The dimensions of the city cops' achievement can be gauged from the fact that they have netted a man who is on the wanted list of the formidable FBI of the United States.

At the time of his detention, he had with him Rs 7.5 lakh knocked off from two ATMs in T Nagar and Abiramipuram in the city. Prior to that, he had walked away with Rs 50,000 from an ATM in Mumbai.

While investigating Manwani's case, the police stumbled upon a cyber crime involving scores of persons across the globe.

Manwani is an MBA drop-out from a Pune college and served as a marketing executive in a Chennai-based firm for some time. Interestingly, his audacious crime career started in an Internet cafe. While browsing the Net one day, he got attracted to a site which offered him assistance in breaking into the ATMs. His contacts, sitting somewhere in Europe, were ready to give him credit card numbers of a few American banks for $5 per card. The site also offered the magnetic codes of those cards, but charged $200 per code.

The operators of the site had devised a fascinating idea to get the personal identification number (PIN) of the card users. They floated a new site which resembled that of a reputed telecom company's. That company has millions of subscribers. The fake site offered the visitors to return $11.75 per head which, the site promoters said, had been collected in excess by mistake from them.

Believing that it was a genuine offer from the telecom company in question, several lakh subscribers logged on to the site to get back that little money, but in the process parted with their PINs.

Armed with all requisite data to hack the bank ATMs, the gang started its systematic looting. Apparently, Manwani and many others of his ilk entered into a deal with the gang behind the site and could purchase any amount of data, of course on certain terms, or simply enter into a deal on a booty-sharing basis.

Meanwhile, Manwani also managed to generate 30 plastic cards that contained necessary data to enable him to break into ATMS.  
  
He was so enterprising that he was able to sell away a few such cards to his contacts in Mumbai. The police are on the lookout for those persons too.

On receipt of large-scale complaints from the billed credit card users and banks in the United States, the FBI started an investigation into the affair and also alerted the CBI in New Delhi that the international gang had developed some links in India too.

Manwani has since been enlarged on bail after interrogation by the CBI. But the city police believe that this is the beginning of the end of a major cyber crime.

**Work at Home scams Exposed**

Cyber Crime Cell of Crime Branch, C.I.D., Mumbai Police have arrested a person by name Sripathi Guruprasanna Raj, aged 52 yrs who is the Chairman and Managing Director of Sohonet India Private Ltd., a company based in Chennai. Many complainants based in Mumbai had complained to the Cyber Crime Investigation Cell, that the said company has duped them each for Rs. 4,000/- and Rs. 6,000/- by promising them with monthly income of Rs. 15,000/-.

**Case of Cyber Extortion**

He does not know much about computer hacking, yet 51-year-old cyber criminal Pranab Mitra has stunned even the cyber crime investigation cell of Mumbai police with his bizarre fraud on the Net. Mitra, a former executive of Gujarat Ambuja Cement, was arrested on Monday for posing as a woman and seducing online an Abu Dhabi-based man,  thereby managing to extort Rs 96 lakh from him. Investigating officer, Assistant Commissioner of Police, J.S. Sodi, said Mitra has been remanded to police custody till June 24, and has been booked for cheating, impersonation, blackmail and extortion under sections 420, 465, 467, 471, 474 of the IPC, read with the newly formed Information Technology Act.

Mitra posed as a woman, Rita Basu, and created a fake e-mail ID through which he contacted one V.R. Ninawe. According to the FIR, Mitra trapped Ninawe in a ‘‘cyber-relationship’’ sending emotional messages and indulging in online **sex** since June 2002.Later, Mitra sent an e-mail that ‘‘she would commit suicide’’ if Ninawe ended the relationship. He also gave him ‘‘another friend Ruchira Sengupta’s’’ e-mail ID which was in fact his second bogus address. When Ninawe mailed at the other ID he was shocked to learn that Mitra had died. Then Mitra began the emotional blackmail by calling up Abu Dhabi to say that police here were searching for Ninawe. Ninawe panicked on hearing the news and asked Mitra to arrange for a good advocate for his defence. Ninawe even deposited a few lakh in the bank as advocate fees. Mitra even sent e-mails as high court and police officials to extort more money. Ninawe finally came down to Mumbai to lodge a police case.

**ICICI Bank Phishing**

Did you know that e-mails, long considered the most convenient form of communication, can actually spring some nasty surprises for you? Recently, a few ICICI Bank customers in Mumbai, to their utter dismay, discovered that e-mails can be extremely hazardous, if not to their health, at least to their security.These ICICI Bank customers received an e-mail from someone who posed as an official of the bank and asked for sensitive information like the account holder's Internet login name and password and directed them to a Web page that resembled the bank's official site.When some customers wrote in to find out what the e-mail was about, the bank officials registered a complaint with the police.

New as it may be in India, it is actually a popular banking scam, a warning against which had been issued by many international banks including Barclays and Citibank. ***rediff.com*** presents a guide that will help readers understand what the scam is about and how they can stay clear of it.

**What happened in the case of the e-mail scam involving ICICI Bank?** A few customers of ICICI Bank received an e-mail asking for their Internet login name and password to their account. The e-mail seemed so genuine that some users even clicked on the URL given in the mail to a Web page that very closely resembled the official site.The scam was finally discovered when an assistant manager of ICICI Bank's information security cell received e-mails forwarded by the bank's customers seeking to crosscheck the validity of the e-mails with the bank. Such a scam is known as 'phishing.'

**Cyber Lotto an Effective Tool of Frauds**

"It is a classic case of cyber crime, the first of its kind in Andhra Pradesh," was how Vijayawada Police Commissioner Sudeep Lakhtakia summed up the case of cheating and fraud registered against Kola Venkata Krishna Mohan, the self-styled winner of the multi-million dollar Euro lottery. Mohan admitted that he did not win the 12.5 million pound Euro lottery in November 1998, as he had claimed, but merely played fraud to make good his losses in gambling.

"With the help of computers, the accused took the people for a ride," the Vijayawada police commissioner pointed out. Mohan, using the Internet and forged documents, allegedly cheated banks and several persons to the tune of 60 million rupees.

Kola Mohan was arrested by the Vijayawada city police on Monday in connection with cases of fraud and forgery registered against him. He was remanded to judicial custody till December 13 by Fifth Metropolitan Magistrate K B Narsimhulu. He was shifted to the district jail at Gandhinagar in Vijayawada. Mohan was accused of cheating the Andhra Bank to the tune of Rs 1.73 million.

By perpetrating the multi-million rupee fraud, Mohan has achieved the dubious distinction of allegedly committing the first and biggest cyber crime in Andhra. The state, incidentally is making rapid strides in information technology, thanks to the initiative of cyber-savvy Chief Minister N Chandrababu Naidu.

A compulsive gambler who played cards regularly at high stakes in various clubs in the coastal city, Mohan told newsmen at the police commissioner's office at Vijayawada on Monday that he had lost as much as Rs 30 million in 1998 when a gambling syndicate led by a real estate dealer and a restaurant-owner cheated him.

"I was on the look-out to make good the losses by hook or crook. During a visit to London, I learnt about the Euro lottery. I staked some money on it in vain. Then, I invented the story that I won the lottery. I created a website and an email address on the Internet with the address 'eurolottery@usa.net.' Whenever accessed, the site would name me as the beneficiary of the 12.5 million pound (that is, $ 19.8 million or Rs 840 million) Euro-lottery," Kola Mohan recalled.

A Telugu newspaper in Hyderabad received an email that a Telugu had won the Euro lottery. The website address was given for verification. The newspaper sent the query and got the "confirmation" since Kola Mohan had himself created and manipulated the website

**Collective Scam in Call Center**

The telemarketing project for an American credit-card company was just coming to an end in January when an internal audit at the Wipro Spectramind call center in Navi Mumbai, India, discovered something very alarming: an organized ring of about 60 call-center agents had been systematically scamming U.S. consumers for two months. Supervisors had told the agents to spice up their sales pitch for the client, Capital One Financial Services, by making false claims about free gifts and membership fees, according to Indian press reports. The scam even bypassed Wipro’s sophisticated call-monitoring system.

**[Reliance made to pay the Consumer](http://economictimes.indiatimes.com/articleshow/1172394.cms)**

 After conducting its own audit, Capital One, located in McLean, Virginia, rescinded the contract with Wipro in March. But its misadventure--and other recent departures from India by U.S. clients--has confirmed many doubts and concerns about the booming business of outsourcing call centers, and also is serving as a catalyst for human resources to develop more effective approaches to managing offshore workers. Experts and consultants believe that companies can meet the challenges and save millions of dollars by improving training and implementing tighter oversight of offshore call agents. Some U.S. companies have even installed their own teams at offshore call centers. "Capital One represents some of the challenges of outsourcing

**Pune BPO-Scam**

Pune BPO scam was claimed to be the first scam in India. In April 2005, five employees of MsourcE in Pune were arrested for allegedly pulling off a fraud worth nearly $425,000 from the Citibank accounts of four New York-based account holders.

**Gurgaon BPO Scam**

In June 2005, the tabloid *Sun* , in a sting operation, purchased the bank account details of 1,000 Britons for about 5.50 dollars companyInfinity E- Search

**Bangalore BPO Scam**

In June 2006, Nadeem Kashmiri sold the customer credit card information to a group of scamsters who used the information to siphon off nearly £233,000 or roughly Rs. 1.8 crore from bank accounts of UK-based customers.

**Data theft makes IT firm quit India**

Published on **Fri, Oct 13, 2006 at 11:48**, **New Delhi:** After registering a case against an employee who had allegedly stolen data, the Gurgaon-based IT firm Acme Telepower Management waited for something to happen. A week later they have decided to stop operating out of India and move to Australia. It seems like this is the beginning of a domino effect, even as India's antiquated police force tries to deal with new age crime like data theft. Acme Telepower is claiming a national loss of Rs 750 crore. They are saying it's all because an ex-employee named Sachidanand Patnaik who allegedly stole research and handed it over to his new employer - a competitor in the power industry solutions space. On Thursday, the board of Acme met after a Gurgaon Sessions court granted bail to Patnaik and decided it was time to pack their bags. "We are disappointed in the system. Patents and research are not protected, so we are not sure if the law will be able to protect us,” GM Marketing, Acme, Sandeep Kashyap said. Acme employs around 1,100 people, who will be affected by the firm’s move to Australia that will happen over the next eight months. Most of the 70 people in the Research and Development section will be the first to move. For the rest, the future is unclear. According to Acme, only a small manufacturing operation will remain in India, but they say they will take care of their employees and that their reason for leaving is simple. "The fact that the main accused has got bail and the others got a clean chit has disappointed us completely,” Kashyap said. However, the lawyer for Sachidanand Patnaik says they are giving up too soon and that this trend could have dangerous repercussions. "If the reason they are leaving India is because the main accused has got bail, then it is contempt of court,” Patnaik's lawyer, Vakul Sharma said. When people lost faith in the system in the past, there was little they could, outside of rallying against everything wrong with the world. However, today people have a choice. They can simply move on. But the question remains - will the system respond?

**Government and Defense sites Attacked and used**

14 May, 2008

Though  
the commercial sectors are the sectors having maximum (85 per cent of total  
defacement in commercial sector) incidents of defacement of government sites,  
which usually have critical information pertaining to security of the country,  
are on continuous rise**. Recently, Defense  
Research and development Organisation (DRDO) site was used to distribute  
malware.**

The  
incidents of defacing government sites are increasing by leaps and bounds. In  
2005 only, 25 government sites were defaced and the number was increased to 70  
in 2006. **In February 2006, websites of  
Government of Punjab were targeted. All the  
websites of Government of Rajasthan were hosted on the same server and in  
November 2006, all the sites were defaced at very short intervals of one to two  
days.** Every year, there is an increase in the total number of website  
defaced in India.  
In 2005 only, 373 deface were reported, which had gone to 1226 in the year  
2006.

**Similar instances**

After Pokhran II test on May 11 – May 13, 1998, a group of hackers called ’Milworm’ broke into Bhabha Atomic Research Centre (BARC) site and posted anti Indian and anti-nuclear messages

In 1999, website of Indian Science  
Congress Association was defaced and the hacker posted provocative comments  
about Kashmir

**Cyber Crime Convictions & Judgments**[**21**](http://satheeshgnair.blogspot.com/#FOOTNOTE-21)

**Case 1: First  
conviction in India**

A complaint was filed in by Sony India Private Ltd, which runs a website called  
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,someone logged onto the website under the identity of Barbara Campa  
and ordered a Sony Colour Television set and a cordless head phone.A lady gave  
her credit card number for payment and requested that the products be delivered  
to Arif Azim in Noida. The payment was duly cleared by the credit card agency  
and the transaction 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 for 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 into 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 head phone.  
  
The accused admitted his guilt and the court of Shri Gulshan Kumar Metropolitan  
Magistrate, New Delhi, convicted Arif Azim under Section 418, 419 and 420 of  
the Indian Penal Code — this being the first time that a cyber crime 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.

**Case-2: First juvenile accused in a cyber crime case.**

In April  2001 a person from New  
Delhi complained to the crime branch regarding the  
website. Amazing.com, he claimed, carried vulgar remarks about his daughter and  
a few of her classmates. During the inquiry, print-outs of the site were taken  
and proceedings initiated.  
  
After investigation a student of Class 11 and classmate of the girl was  
arrested.  
  
 The juvenile board in Nov 2003 refused to discharge the boy accused of  
creating a website with vulgar remarks about his classmate.  
  
The accused’s advocate had sought that his client be discharged on the ground  
that he was not in a stable state of mind. Seeking discharge, the advocate  
further said that the trial has been pending for about two years.  
  
While rejecting the accused’s application, metropolitan magistrate Santosh  
Snehi Mann said: ‘The mental condition under which the juvenile came into  
conflict with the law shall be taken into consideration during the final  
order.’ Mann, however, dropped the sections of Indecent Representation of Women  
(Prohibition) Act.  
  
The accused would face trial under the Information Technology Act and for  
intending to outrage the modesty of a woman. She held the inquiry could not be  
closed on technical ground, especially when the allegations were not denied by  
the accused.

**Case 3: First case convicted under Information Technology Act 2000 of 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 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 a complaint made by the victim in February 2004,  the Police  
traced the accused to Mumbai and arrested him within the next few days.   
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.  
  
On 24-3-2004 Charge Sheet was filed u/s 67 of IT Act 2000, 469 and 509 IPC  
before The Hon’ble Addl. CMM Egmore by citing 18 witnesses and 34 documents and  
material objects. The same was taken on file in C.C.NO.4680/2004.  On the  
prosecution side 12 witnesses were examined and entire documents were marked.  
 The Defence argued that the offending mails would have been given either  
by ex-husband of the complainant or the complainant her self to implicate the  
accused as accused alleged to have turned down the request of the complainant  
to marry her.  Further the Defence counsel argued that some of the  
documentary evidence was not sustainable under Section 65 B of the Indian  
Evidence Act.  However, the court based on the expert witness of Naavi and  
other evidence produced including the witness of the Cyber Cafe owners came to  
the conclusion that the crime was conclusively proved.  
  
The court has also held  that because of the meticulous   
investigation carried on by the IO, the origination of the obscene message was  
traced out and the real culprit has been brought before the court of law.   
In this case Sri S. Kothandaraman, Special Public Prosecutor appointed by the  
Government conducted the case.  
  
Honourable Sri.Arulraj, Additional Chief Metropolitan Magistrate, Egmore,  
delivered the judgement on 5-11-04 as follows:  
  
“The accused is found guilty of offences under section 469, 509 IPC and 67 of  
IT Act 2000 and the accused is convicted and is sentenced for the offence to  
undergo RI for 2 years under 469 IPC and to pay fine of Rs.500/-and for the  
offence u/s 509 IPC sentenced to undergo 1 year Simple imprisonment and to pay  
fine of Rs.500/- and for the offence u/s 67 of IT Act 2000  to undergo RI  
for 2 years and to pay fine of Rs.4000/-  All sentences to run concurrently.”

**Case 4: Father & son convicted under IT act in Kerala.**

The Additional District and Sessions Court here has upheld a lower court’s  
verdict in the first cyber case filed in the State sentencing a Pentecostal Church priest and his son to rigorous  
imprisonment in 2006.  
  
Disposing of the appeal filed by the priest T.S. Balan and his son, Aneesh  
Balan, against the order of the Chief Judicial Magistrate, on Wednesday,  
  
Additional District Judge T.U. Mathewkutty said it was time the government took  
effective measures to check the growing trend of cyber crimes in the State.The  
court upheld the magistrate’s order sentencing the two to three-year rigorous  
imprisonment and imposing a fine of Rs. 25,000 under Section 67 of the  
information technology (IT) Act; awarding six months rigorous imprisonment  
under Section 120(B) of the Indian Penal Code; and ordering one year rigorous  
imprisonment and imposing a fine of Rs. 10,000 under Section 469 of the code.  
  
The court revoked the sentence under Section 66 of the IT Act.  
  
The cyber case dates back to January-February 2002 and the priest and his son  
became the first to be convicted of committing a cyber crime.  
  
The two were found guilty of morphing, web-hosting and e-mailing nude pictures  
of Pastor Abraham and his family.  
  
Balan had worked with the pastor until he fell out with him and was shown the  
door by the latter.  
  
Balan joined the Sharon  
Pentecostal Church  
later.  
  
The prosecution said the duo had morphed photographs of Abraham, his son,  
Valsan Abraham, and daughter, Starla Luke, and e-mailed them from fake mail IDs  
with captions.  
  
The morphed pictures were put on the web and the accused, who edited a local  
magazine called The Defender, wrote about these photos in his publication.  
  
Valsan received the pictures on the Internet and asked his father to file a  
complaint to the police. A police party raided the house of Balan and his son  
at Perumbavoor and collected evidences.  
  
The magistrate’s verdict came after a four-year trial, for which the court had  
to procure a computer with Internet connection and accessories.  
  
The police had to secure the services of a computer analyst too to piece  
together the evidences. Twenty-nine witnesses, including the Internet service  
provider and Bharat Sanchar Nigam Ltd., had to depose before the court.

**Case 5: Well-known orthopedist 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 doctor 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.  
  
Subsequent police investigations opened up a Pandora's box. Prakash and his  
younger brother, settled in the US,  
had piled up close to one lakh shots and video footages, some real and many  
morphed.  
  
They reportedly minted huge money in the porn business, it was stated.  
  
Fast track court judge R Radha, who convicted all the four in Feb 2008 , also  
imposed a fine of Rs 1.27 lakh on Prakash, the main accused in the case, and Rs  
2,500 each on his three associates - Saravanan, Vijayan and Asir Gunasingh.  
  
The Judge while awarding life term to Prakash observed that considering the  
gravity of the offences committed by the main accused, maximum punishment under  
the Immoral Trafficking Act (life imprisonment) should be given to him and no  
leniency should be shown.  
  
The Judge sentenced Prakash under the Immoral Trafficking Act, IPC, Arms Act  
and Indecent Representation of Women (Prevention) Act among others.

**Case 6:Juvenile found guilty for sending threatening email.**

A 16 year old student from Ahmadabad who threatened to blow up Andheri Railway  
station in an email message was found guilty by the Juvenile court in Mumbai.  
  
A private news channel received an email on 18 March 2008 claiming sender as  
Dawood Ibrahim gang saying a bomb would be planted on an unspecified train to  
blow it up.  
  
The case was registered in Andheri Police station under section 506 of IPC and  
transferred to cyber crime investigation cell. During Investigation CCIC traced  
the cyber cafe from which the email account was created and threatening email  
was sent.  
  
Cafe owner told police about friends which had come that day to surf the  
net.Police Summoned them and found that the system which was used to send email  
was accessed by only one customer. On 22nd March 08, police arrested the  
boy a Class XII science student who during interrogation said that he sent the  
email for fun of having his prank flashed as “breaking news’’ on  
television.