Real world

cyber crime cases

This document is an extract from the book *Cyber Crime & Digital Evidence – Indian Perspective* authored by Rohas Nagpal. This book is available as courseware for the **Diploma in Cyber Law** and **PG Program in Cyber Law** conducted by Asian School of Cyber Laws

www.asianlaws.org

23. Real World Cases

This chapter serves as a ready reference guide. First the various scenarios are covered.

A detailed discussion on the various cyber crimes, is covered in the ASCL publication titled "**Understanding Hackers and Cyber Criminals**".

This is provided as official courseware for the ASCL Certified Cyber Crime Investigator course.

Then the applicable law and legal liabilities are covered. Then the modus operandi usually followed by the criminals is discussed.

The investigation guidelines for cyber crime investigators are not discussed in this book as they are part of the syllabus of the ASCL Certified Cyber Crime Investigator course only.

For real world case studies on investigation of cyber crimes, please refer to the ASCL publication titled "**Case Studies on Cyber Crime Investigation**".

This is provided as official courseware for the ASCL Certified Cyber Crime Investigator course.

© 2008 Rohas Nagpal. All rights reserved.

23.1 Orkut Fake Profile cases

Orkut.com is a very popular online community and social networking website. Orkut users can search for and interact with people who share the same hobbies and interests. They can create and join a wide variety of online communities. The profiles of Orkut members are publicly viewable.

The scenarios

1. A **fake profile of a woman is created** on Orkut. The profile displays her correct name and contact information (such as address, residential phone number, cell phone number etc). Sometimes it even has her photograph.

   The problem is that the profile describes her as a prostitute or a woman of "loose character" who wants to have sexual relations with anyone. Other Orkut members see this profile and start calling her at all hours of the day asking for sexual favours. This leads to a lot of harassment for the victim and also defames her in society.

2. An **online hate community** is created. This community displays objectionable information against a particular country, religious or ethnic group or even against national leaders and historical figures.

3. A **fake profile of a man is created** on Orkut. The profile contains defamatory information abut the victim (such as his alleged sexual weakness, alleged immoral character etc)

The law

Scenario 1: Section 67 of Information Technology Act and section 509 of the Indian Penal Code.

Scenario 2: Section 153A and 153B of Indian Penal Code.

Scenario 3: Section 500 of Indian Penal Code.

Who is liable?

Scenario 1: Directors of Orkut as well as all those who create and update the fake profile.

Scenario 2: Same as Scenario 1.

Scenario 3: Same as Scenario 1.

© 2008 Rohas Nagpal. All rights reserved.

The motive

Scenario 1: Jealousy or revenge (e.g. the victim may have rejected the advances made by the suspect).

Scenario 2: Desire to cause racial hatred (e.g. Pakistani citizens creating an anti-India online community).

Scenario 3: Hatred (e.g. a school student who has failed may victimize his teachers).

Modus Operandi

1. The suspect would create a free Gmail account using a fictitious name.
2. The email ID chosen by him would be unrelated to his real identity.
3. The suspect would then login to Orkut.com and create the offensive profile.

© 2008 Rohas Nagpal. All rights reserved.

23.2 Email Account Hacking

Emails are increasingly being used for social interaction, business communication and online transactions. Most email account holders do not take basic precautions to protect their email account passwords. Cases of theft of email passwords and subsequent misuse of email accounts are becoming very common.

The scenarios

1. The victim's email account password is stolen and the account is then misused for sending out malicious code (virus, worm, Trojan etc) to people in the victim's address book. The recipients of these viruses believe that the email is coming from a known person and run the attachments. This infects their computers with the malicious code.

2. The victim's email account password is stolen and the hacker tries to extort money from the victim. The victim is threatened that if he does not pay the money, the information contained in the emails will be misused.

3. The victim's email account password is stolen and obscene emails are sent to people in the victim's address book.

The law

Scenario 1: Sections 43 and 66 of Information Technology Act.

Scenario 2: Sections 43 and 66 of Information Technology Act and section 384 of Indian Penal Code.

Scenario 3: Sections 43, 66 and 67 of Information Technology Act and section 509 of the Indian Penal Code.

Who is liable?

Scenario 1: Persons who have stolen the email account password and who are misusing the email account.

Scenario 2: Persons who have stolen the email account password and who are threatening to misuse it.

© 2008 Rohas Nagpal. All rights reserved.

Scenario 3: Persons who have stolen the email account password and who are misusing the email account.

The motive

Scenario 1: Corporate Espionage, perverse pleasure in being able to destroy valuable information belonging to strangers etc.

Scenario 2: Illegal financial gain.

Scenario 3: Revenge, jealousy, hatred.

Modus Operandi

1. The suspect would install keyloggers in public computers (such as cyber cafes, airport lounges etc) or the computers of the victim.

2. Unsuspecting victims would login to their email accounts using these infected computers.

3. The passwords of the victim's email accounts would be emailed to the suspect.

© 2008 Rohas Nagpal. All rights reserved.

23.3 Credit Card Fraud

Credit cards are commonly being used for online booking of airline and railway tickets and for other ecommerce transactions. Although most of ecommerce websites have implemented strong security measures (such as SSL, secure web servers etc), instances of credit card frauds are increasing.

The scenario

The victim's credit card information is stolen and misused for making online purchases (e.g. airline tickets, software, subscription to pornographic websites etc).

The law

Sections 43 and 66 of Information Technology Act and section 420 of Indian Penal Code.

Who is liable?

All persons who have stolen the credit card information as well as those who have misused it.

The motive

Illegal financial gain.

Modus Operandi

Scenario 1: The suspect would install keyloggers in public computers (such as cyber cafes, airport lounges etc) or the computers of the victim. Unsuspecting victims would use these infected computers to make online transactions. The credit card information of the victim would be emailed to the suspect.

Scenario 2: Petrol pump attendants, workers at retail outlets, hotel waiters etc note down information of the credit cards used for making payment at these establishments. This information is sold to criminal gangs that misuse it for online frauds.

© 2008 Rohas Nagpal. All rights reserved.

23.4 Online Share Trading Fraud

With the advent of dematerialization of shares in India, it has become mandatory for investors to have demat accounts. In most cases an online banking account is linked with the share trading account. This has led to a high number of online share trading frauds.

The scenario

Scenario 1: The victim's account passwords are stolen and his accounts are misused for making fraudulent bank transfers.

Scenario 2: The victim's account passwords are stolen and his share trading accounts are misused for making unauthorised transactions that result in the victim making losses.

The law

Scenario 1: Sections 43 and 66 of Information Technology Act and section 420 of Indian Penal Code.

Scenario 2: Sections 43 and 66 of Information Technology Act and section 426 of Indian Penal Code.

Who is liable?

Scenario 1: All persons who have stolen the account information as well as those who have misused it.

Scenario 2: All persons who have stolen the account information as well as those who have misused it.

The motive

Scenario 1: Illegal financial gain

Scenario 2: Revenge, jealousy, hatred

Modus Operandi

Scenario 1: The suspect would install keyloggers in public computers (such as cyber cafes, airport lounges etc) or the computers of the victim. Unsuspecting victims would use these infected computers to login to their online banking and share trading accounts. The passwords and other information of the victim would be emailed to the suspect.

Scenario 2: Same as scenario 1.

© 2008 Rohas Nagpal. All rights reserved.

23.5 Tax Evasion and Money Laundering

Many unscrupulous businessmen and money launderers (havala operators) are using virtual as well as physical storage media for hiding information and records of their illicit business.

The scenario

Scenario 1: The suspect uses physical storage media for hiding the information e.g. hard drives, floppies, USB drives, mobile phone memory cards, digital camera memory cards, CD ROMs, DVD ROMs, iPods etc.

Scenario 2: The suspect uses virtual storage media for hiding the information e.g. email accounts, online briefcases, FTP sites, Gspace etc.

The law

Scenario 1: Depending upon the case, provisions of the Income Tax Act and Prevention of Money Laundering Act will apply.

Scenario 2: Depending upon the case, provisions of the Income Tax Act and Prevention of Money Laundering Act will apply.

Who is liable?

Scenario 1: The person who hides the information.

Scenario 2: The person who hides the information. If the operators of the virtual storage facility do not cooperate in the investigation, then they also become liable.

The motive

Scenario 1: Illegal financial gain

Scenario 2: Illegal financial gain

Modus Operandi

Scenario 1: The suspect would purchase small storage devices with large data storage capacities.

Scenario 2: The suspect would open free or paid accounts with online storage providers.

© 2008 Rohas Nagpal. All rights reserved.

23.6 Source Code Theft

Computer source code is the most important asset of software companies. Simply put, source code is the programming instructions that are compiled into the executable files that are sold by software development companies.

As is expected, most source code thefts take place in software companies. Some cases are also reported in banks, manufacturing companies and other organisations who get original software developed for their use.

The scenario

Scenario 1: The suspect (usually an employee of the victim) steals the source code and sells it to a business rival of the victim.

Scenario 2: The suspect (usually an employee of the victim) steals the source code and uses it as a base to make and sell his own version of the software.

The law

Scenario 1: Sections 43, 65 and 66 of the Information Technology Act, section 63 of the Copyright Act.

Scenario 2: Sections 43, 65 and 66 of the Information Technology Act, section 63 of the Copyright Act.

Who is liable?

Scenario 1: The persons who steal the source code as well as the persons who purchase the stolen source code.

Scenario 2: The persons who steal the source code.

The motive

Scenario 1: Illegal financial gain.

Scenario 2: Illegal financial gain.

Modus Operandi

Scenario 1: If the suspect is an employee of the victim, he would usually have direct or indirect access to the source code. He would steal a copy of the source code and hide it using a virtual or physical storage device.

© 2008 Rohas Nagpal. All rights reserved.

If the suspect is not an employee of the victim, he would hack into the victim's servers to steal the source code. Or he would use social engineering to get unauthorised access to the code.

He would then contact potential buyers to make the sale.

Scenario 2: If the suspect is an employee of the victim, he would usually have direct or indirect access to the source code. He would steal a copy of the source code and hide it using a virtual or physical storage device.

If the suspect is not an employee of the victim, he would hack into the victim's servers to steal the source code. Or he would use social engineering to get unauthorised access to the code.

He would then modify the source code (either himself or in association with other programmers) and launch his own software.

© 2008 Rohas Nagpal. All rights reserved.

23.7 Theft of Confidential Information

Most business organisations store their sensitive information in computer systems. This information is targeted by rivals, criminals and sometimes disgruntled employees.

The scenario

Scenario 1: A business rival obtains the information (e.g. tender quotations, business plans etc) using hacking or social engineering. He then uses the information for the benefit of his own business (e.g. quoting lower rates for the tender).

Scenario 2: A criminal obtains the information by hacking or social engineering and threatens to make the information public unless the victim pays him some money.

Scenario 3: A disgruntled employee steals the information and mass mails it to the victim's rivals and also posts it to numerous websites and newsgroups.

The law

Scenario 1: Sections 43 and 66 of the Information Technology Act, section 426 of Indian Penal Code.

Scenario 2: Sections 43 and 66 of the Information Technology Act, section 384 of Indian Penal Code.

Scenario 3: Sections 43 and 66 of the Information Technology Act, section 426 of Indian Penal Code.

Who is liable?

Scenario 1: The persons who steal the information as well as the persons who misuse the stolen information.

Scenario 2: The persons who steal the information as well as the persons who threaten the victim and extort money.

Scenario 3: The disgruntled employee as well as the persons who help him in stealing and distributing the information.

The motive

Scenario 1: Illegal financial gain.

Scenario 2: Illegal financial gain.

Scenario3: Revenge.

© 2008 Rohas Nagpal. All rights reserved.

Modus Operandi

Scenario 1: The suspect could hire a skilled hacker to break into the victim systems. The hacker could also use social engineering techniques.

Illustration:
A very good looking woman went to meet the system administrator (sysadmin) of a large company. She interviewed the sysadmin for a "magazine article".

During the interview she flirted a lot with the sysadmin and while leaving she "accidentally" left her pen drive at the sysadmin's room.

The sysadmin accessed the pen drive and saw that it contained many photographs of the lady. He did not realize that the photographs were Trojanized!

Once the Trojan was in place, a lot of sensitive information was stolen very easily.

Illustration:
The sysadmin of a large manufacturing company received a beautifully packed CD ROM containing "security updates" from the company that developed the operating system that ran his company's servers.

He installed the "updates" which in reality were Trojanized software. For 3 years after that a lot of confidential information was stolen from the company's systems!

Scenario 2: Same as scenario 1.

Scenario 3: The disgruntled employee would usually have direct or indirect access to the information. He can use his personal computer or a cyber café to spread the information.

© 2008 Rohas Nagpal. All rights reserved.

23.8 Software Piracy

Many people do not consider software piracy to be theft. They would never steal a rupee from someone but would not think twice before using pirated software. There is a common perception amongst normal computer users to not consider software as “property”.

This has led to software piracy becoming a flourishing business.

The scenario

Scenario 1: The software pirate sells the pirated software in physical media (usually CD ROMs) through a close network of dealers.

Scenario 2: The software pirate sells the pirated software through electronic downloads through websites, bulletin boards, newsgroups, spam emails etc.

The law

Scenario 1: Sections 43 and 66 of the Information Technology Act, section 63 of Copyright Act.

Scenario 2: Sections 43 and 66 of the Information Technology Act, section 63 of Copyright Act.

Who is liable?

Scenario 1: The software pirate as well as the persons who buy the pirated software from him.

Scenario 2: The software pirate as well as the persons who buy the pirated software from him.

The motive

Scenario 1: Illegal financial gain.

Scenario 2: Illegal financial gain.

Modus Operandi

Scenario 1: The suspect uses high speed CD duplication equipment to create multiple copies of the pirated software. This software is sold through a network of computer hardware and software vendors.

Scenario 2: The suspect registers a domain name using a fictitious name and then hosts his website using a service provider that is based in a country that does not have cyber laws. Such service providers do not divulge client information to law enforcement officials of other countries.

© 2008 Rohas Nagpal. All rights reserved.

23.9 Music Piracy

Many people do not consider music piracy to be theft. They would never steal a rupee from someone but would not think twice before buying or using pirated music. There is a common perception amongst people users to not consider music as “property”. There is a huge business in music piracy. Thousands of unscrupulous businessmen sell pirated music at throw away prices.

The scenario

Scenario 1: The music pirate sells the pirated music in physical media (usually CD ROMs) through a close network of dealers.

Scenario 2: The music pirate sells the pirated music through electronic downloads through websites, bulletin boards, newsgroups, spam emails etc.

The law

Scenario 1: Sections 43 and 66 of the Information Technology Act, section 63 of Copyright Act.

Scenario 2: Sections 43 and 66 of the Information Technology Act, section 63 of Copyright Act.

Who is liable?

Scenario 1: The music pirate as well as the persons who buy the pirated software from him.

Scenario 2: The music pirate as well as the persons who buy the pirated software from him.

The motive

Scenario 1: Illegal financial gain.

Scenario 2: Illegal financial gain.

Modus Operandi

Scenario 1: The suspect uses high speed CD duplication equipment to create multiple copies of the pirated music. This music is sold through a network of dealers.

Scenario 2: The suspect registers a domain name using a fictitious name and then hosts his website using a service provider that is based in a country that does not have cyber laws. Such service providers do not divulge client information to law enforcement officials of other countries.

© 2008 Rohas Nagpal. All rights reserved.

23.10 Email Scams

Emails are fast emerging as one of the most common methods of communication in the modern world. As can be expected, criminals are also using emails extensively for their illicit activities.

The scenario

In the first step, the suspect convinces the victim that the victim is going to get a lot of money (by way of winning a lottery or from a corrupt African bureaucrat who wants to transfer his ill gotten gains out of his home country). In order to convince the victim, the suspect sends emails (some having official looking documents as attachments).

Once the victim believes this story, the suspect asks for a small fee to cover legal expenses or courier charges. If the victim pays up the money, the suspect stops all contact.

The law

Section 420 of Indian Penal Code

Who is liable?

The sender of the email.

The motive

Illegal financial gain.

Modus Operandi

The suspect creates email accounts in fictitious names and sends out millions of fraudulent emails using powerful spam software.

© 2008 Rohas Nagpal. All rights reserved.

23.11 Phishing

With the tremendous increase in the use of online banking, online share trading and ecommerce, there has been a corresponding growth in the incidents of phishing being used to carry out financial frauds.

Phishing involves fraudulently acquiring sensitive information (e.g. passwords, credit card details etc) by masquerading as a trusted entity.

The scenario

Scenario 1: The victim receives an email that appears to have been sent from his bank. The email urges the victim to click on the link in the email. When the victim does so, he is taken to "a secure page on the bank's website".

The victim believes the web page to be authentic and he enters his username, password and other information. In reality, the website is a fake and the victim's information is stolen and misused.

The law

Sections 43 and 66 of Information Technology Act and sections 419, 420 and 468 of Indian Penal Code.

Who is liable?

All persons involved in creating and sending the fraudulent emails and creating and maintaining the fake website. The persons who misuse the stolen or "phished" information are also liable.

The motive

Illegal financial gain.

Modus Operandi

The suspect registers a domain name using fictitious details. The domain name is usually such that can be misused for spoofing e.g. Noodle Bank has its website at www.noodle.com The suspects can target Noodle customers using a domain name like www.noodle-bank-customerlogin.com

The suspect then sends spoofed emails to the victims. e.g. the emails may appear to come from info@noodle.com

The fake website is designed to look exactly like the original website.

© 2008 Rohas Nagpal. All rights reserved.

23.12 Cyber Pornography

Cyber pornography is believed to be one of the largest businesses on the Internet today. The millions of pornographic websites that flourish on the Internet are testimony to this. While pornography per se is not illegal in many countries, child pornography is strictly illegal in most nations today.

Cyber pornography includes pornographic websites, pornographic magazines produced using computers (to publish and print the material) and the Internet (to download and transmit pornographic pictures, photos, writings etc).

The scenario

The suspect accepts online payments and allows paying customers to view / download pornographic pictures, videos etc from his website.

The law

Section 67 of Information Technology Act.

Who is liable?

The persons who create and maintain the pornographic websites are liable. In some cases cyber café owners and managers may also be liable in case they knowingly allow their customers to access the pornographic websites.

The motive

Illegal financial gain.

Modus Operandi

The suspect registers a domain name using fictitious details and hosts a website on a server located in a country where cyber pornography is not illegal.

The suspect accepts online payments and allows paying customers to view / download pornographic pictures, videos etc from his website.

© 2008 Rohas Nagpal. All rights reserved.

23.13 Online Sale of Illegal Articles

It is becoming increasingly common to find cases where sale of narcotics drugs, weapons, wildlife etc. is being facilitated by the Internet. Information about the availability of the products for sale is being posted on auction websites, bulletin boards etc.

The scenario

The suspect posts information about the illegal sale that he seeks to make. Potential customers can contact the seller using the email IDs provided. If the buyer and seller trust each other after their email and / or telephonic conversation, the actual transaction can be concluded. In most such cases the buyer and seller will meet face to face at the time of the final transaction.

Illustration:
In March 2007, the Pune rural police cracked down on an illegal rave party and arrested hundreds of illegal drug users. The social networking site, Orkut.com, is believed to be one of the modes of communication for gathering people for the illegal “drug” party.

The law

Depending upon the illegal items being transacted in, provisions of the Narcotic Drugs and Psychotropic Substances Act, Arms Act, Indian Penal Code, Wildlife related laws etc may apply.

Who is liable?

The persons who buy and sell these items.

The motive

Illegal financial gain.

Modus Operandi

The suspect creates an email ID using fictitious details. He then posts messages, about the illegal products, in various chat rooms, bulletin boards, newsgroups etc. Potential customers can contact the seller using the email IDs provided.

If the buyer and seller trust each other after their email and / or telephonic conversation, the actual transaction can be concluded. In most such cases the buyer and seller will meet face to face at the time of the final transaction.

© 2008 Rohas Nagpal. All rights reserved.

23.14 Use of Internet and Computers by Terrorists

Many terrorists are using virtual as well as physical storage media for hiding information and records of their illicit business. They also use emails and chat rooms to communicate with their counterparts around the globe.

The scenario

The suspects carry laptops wherein information relating to their activities is stored in encrypted and password protected form. They also create email accounts using fictitious details. In many cases, one email account is shared by many people.

E.g. one terrorist composes an email and saves it in the draft folder. Another terrorist logs into the same account from another city / country and reads the saved email. He then composes his reply and saves it in the draft folder. The emails are not actually sent. This makes email tracking and tracing almost impossible.

Terrorists also use physical storage media for hiding the information e.g. hard drives, floppies, USB drives, mobile phone memory cards, digital camera memory cards, CD ROMs, DVD ROMs, iPods etc. They also use virtual storage media for hiding the information e.g. email accounts, online briefcases, FTP sites, Gspace etc.

The law

Terrorists are covered by conventional laws such as Indian Penal Code and special legislation relating to terrorism.

Who is liable?

Terrorists as well as those who help them to protect their information are liable. If email service providers do not assist the law enforcement personnel in the investigation then they are also legally liable.

The motive

Keeping terrorism related information confidential.
Secure communication amongst terrorist group members.

Modus Operandi

The terrorists purchase small storage devices with large data storage capacities. They also purchase and use encryption software. The terrorists may also use free or paid accounts with online storage providers.

© 2008 Rohas Nagpal. All rights reserved.

23.15 Virus Attacks

Computer viruses are malicious programs that destroy electronic information. As the world is increasingly becoming networked, the threat and damage caused by viruses is growing by leaps and bounds.

The scenario

Scenario 1: The virus is a general "in the wild" virus. This means that it is spreading all over the world and is not targeted at any specific organisation.

Scenario 2: The virus targets a particular organisation. This type of a virus is not known to anti-virus companies as it is a new virus created specifically to target a particular organisation.

The law

Scenario 1: Sections 43 and 66 of Information Technology Act and section 426 of Indian Penal Code.

Scenario 2: Sections 43 and 66 of Information Technology Act and section 426 of Indian Penal Code.

Who is liable?

Scenario 1: The creator of the virus.

Scenario 2: The creator of the virus as well as the buyer who purchases the virus (usually to target his business rivals).

The motive

Scenario 1: Thrill and a perverse pleasure in destroying data belonging to strangers.

Scenario 2: Illegal financial gain, revenge, business rivalry.

Modus Operandi

Scenario 1: A highly skilled programmer creates a new type or strain of virus and releases it on the Internet so that it can spread all over the world.

Being a new virus, it goes undetected by many anti-virus software and hence is able to spread all over the world and cause a lot of damage.

Anti-virus companies are usually able to find a solution within 8 to 48 hours.

© 2008 Rohas Nagpal. All rights reserved.

Scenario 2: A highly skilled programmer creates a new type or strain of virus. He does not release it on the Internet. Instead he sells it for a huge amount of money.

The buyer uses the virus to target his rival company. Being a new virus, it may be undetected by the victim company's anti-virus software and hence would be able to cause a lot of damage.

Anti-virus companies may never get to know about the existence of the virus.

© 2008 Rohas Nagpal. All rights reserved.

23.16 Web Defacement

Website defacement is usually the substitution of the original home page of a website with another page (usually pornographic or defamatory in nature) by a hacker.

Religious and government sites are regularly targeted by hackers in order to display political or religious beliefs. Disturbing images and offensive phrases might be displayed in the process, as well as a signature of sorts, to show who was responsible for the defacement. Websites are not only defaced for political reasons, many defacers do it just for the thrill.

The scenario

The homepage of a website is replaced with a pornographic or defamatory page. In case of Government websites, this is most commonly done on symbolic days (e.g. the Independence day of the country).

The law

Sections 43 and 66 of Information Technology Act [In some cases section 67 and 70 may also apply].

Who is liable?

The person who defaces the website.

The motive

Thrill or a perverse pleasure in inciting communal disharmony.

Modus Operandi

The defacer may exploit the vulnerabilities of the operating system or applications used to host the website. This will allow him to hack into the web server and change the home page and other pages.

Alternatively he may launch a brute force or dictionary attack to obtain the administrator passwords for the website. He can then connect to the web server and change the webpages.

© 2008 Rohas Nagpal. All rights reserved.

www.asianlaws.org

Head Office

6th Floor, Pride Senate,

Behind Indiabulls Mega Store,

Senapati Bapat Road,

Pune - 411016.

India

Contact Numbers

+91-20-25667148

+91-20-40033365

+91-20-64000000

+91-20-64006464

Email: info@asianlaws.org

URL: www.asianlaws.org