

Free copy



# EVOLUTION OF CYBER CRIME

**data64**

Techno Solutions Pvt. Ltd.



# Evolution of **CYBER CRIME**

**Published in 2009 by Data64 Techno Solutions Pvt Ltd**

**Copy right © 2009 by Rohas Nagpal. All rights reserved.**

No part of this book may be reproduced or otherwise used without prior written permission from the author unless such use is expressly permitted by applicable law.

No investigation has been made of common-law trademark rights in any word. Words that are known to have current trademark registrations are shown with an initial capital and are also identified as trademarks.

The inclusion or exclusion of any word, or its capitalization, in this book is not, however, an expression of the publisher's opinion as to whether or not it is subject to proprietary rights, nor is it to be regarded as affecting the validity of any trademark.

This book is provided "as is" and Data64 Techno Solutions Pvt Ltd makes no representations or warranties, express or implied either in respect of this book or the software, websites and other information referred to in this book.

By way of example, but not limitation, Data64 Techno Solutions Pvt Ltd makes no representations or warranties of merchantability or fitness for any particular purpose or that the use of licensed software, database or documentation will not infringe any third party patents, copyrights, trademarks or other rights.

**Printed in India**

**The chosen case scenarios are for instructional purposes only and any association to an actual case and litigation is purely coincidental. Names and locations presented in the case scenarios are fictitious and are not intended to reflect actual people or places.**

**Reference herein to any specific commercial products, processes, or services by trade name, trademark, manufacturer, or otherwise does not constitute or imply its endorsement, recommendation, or favoring by Data64 Techno Solutions Pvt Ltd, and the information and statements shall not be used for the purposes of advertising.**



## About the Author

**Rohas Nagpal** is the founder President of Asian School of Cyber Laws. He advises Governments and corporates around the world in cyber crime investigation and cyber law related issues. He has assisted the Government of India in drafting rules and regulations under the Information Technology Act, 2000.

He has authored several books, papers and articles on cyber law, cyber terrorism, cyber crime investigation and financial law.

Rohas lives in Pune (India) and blogs @ rohasnagpal.com

### **Some of the papers authored by Rohas Nagpal**

1. Internet Time Theft & the Indian Law
2. Legislative Approach to Digital Signatures
3. Indian Legal Position on Cyber Terrorism
4. Defining Cyber Terrorism
5. The Mathematics of Terror
6. Cyber Terrorism in the context of Globalization
7. Biometric based Digital Signature Scheme



### Director's Message

Dear Reader,

Over the years in my interaction with students, educational institutions, law enforcement agencies and corporate houses I have realized that a growing number of people are **e-connected** but not really **e-aware**.

Accordingly, we took our first step in making people cyber aware by publishing this book entitled '**Evolution of Cyber Crime**'.

This simple illustration driven book gives a birds eye view of the various forms of cyber crimes.

Another initiative taken by us is the Data64 blog available @ [www.data64.com/blog](http://www.data64.com/blog). The blog takes you through various hacking and security issues, cyber related cases, latest tech gadgets and news and initiatives taken by people to eradicate cyber crime.

I hope you enjoy reading the book and the blog.

*Gokul Narayan*

**Gokul Narayan**  
Director  
Data64 Techno Solutions Pvt. Ltd.

**Table of Contents**

Chapter 1 Evolution of Cyber Crimes .....	6
Chapter 2 Financial Crimes .....	7
Chapter 3 Cyber Pornography .....	8
Chapter 4 Sale of Illegal Articles.....	9
Chapter 5 Online Gambling .....	10
Chapter 6 Intellectual Property Crimes.....	11
Chapter 7 Email Spoofing .....	12
Chapter 8 Forgery .....	13
Chapter 9 Cyber Defamation.....	14
Chapter 10 Cyber Stalking.....	15
Chapter 11 Web Defacement.....	16
Chapter 12 Email Bombing.....	17
Chapter 13 Data Diddling.....	18
Chapter 14 Salami Attacks .....	19
Chapter 15 Denial of Service Attacks .....	20
Chapter 16 Virus / Worm Attacks .....	21
Chapter 17 Trojans and Keyloggers .....	23
Chapter 18 Internet Time Theft.....	24
Chapter 19 Web Jacking.....	25
Chapter 20 Email Frauds .....	27
Chapter 21 Cyber Terrorism.....	30
Chapter 22 Use of Encryption by Terrorists.....	31

## Chapter 1 Evolution of Cyber Crimes

The first **recorded cyber crime** took place in the year **1820!** That is not surprising considering the fact that the abacus, which is thought to be the earliest form of a computer, has been around since 3500 B.C. in India, Japan and China. The era of modern computers, however, began with the analytical engine of Charles Babbage.

In 1820, **Joseph-Marie Jacquard**, a textile manufacturer in France, produced the loom. This device allowed the repetition of a series of steps in the weaving of special fabrics. This resulted in a fear amongst Jacquard's employees that their traditional employment and livelihood were being threatened. They committed acts of sabotage to discourage Jacquard from further use of the new technology. This is the **first recorded cyber crime!**

Today, computers have come a long way with **neural networks and nanocomputing** promising to turn every atom in a glass of water into a computer capable of performing a billion operations per second. In a day and age when everything from microwave ovens and refrigerators to nuclear power plants are being run on computers, cyber crime has assumed rather sinister implications.

Cyber crime can involve criminal activities that are **traditional** in nature, such as theft, fraud, forgery, defamation and mischief. The abuse of computers has also given birth to a gamut of **new age crimes** such as hacking, web defacement, cyber stalking, web jacking etc.

A simple yet sturdy **definition of cyber crime** would be:

***“unlawful acts wherein the computer is either a tool or a target or both”.***

The **term computer used in this definition** does not only mean the conventional desktop or laptop computer. It includes Personal Digital Assistants (PDA), cell phones, sophisticated watches, cars and a host of gadgets.

## Chapter 2 Financial Crimes

Money is the most common motive behind all crime. The same is also true for cyber crime.

Globally it is being observed that more and more cyber crimes are being committed for financial motives rather than for “**revenge**” or for “**fun**”. With the tremendous increase in the use of internet and mobile banking, online share trading, dematerialization of shares and securities, this trend is likely to increase unabated.

**Financial crimes** include cyber cheating, credit card frauds, money laundering, hacking into bank servers, computer manipulation, accounting scams etc.

### Illustration 1

Punjab National Bank in India was cheated to the tune of Rs. 13.9 million through false debits and credits in computerized accounts.

### Illustration 2

Rs. 2,50,000 were misappropriated from Bank of Baroda in India through falsification of computerized bank accounts.

### Illustration 3

The Hyderabad police in India arrested an unemployed computer operator and his friend, a steward in a prominent five-star hotel, for stealing and misusing credit card numbers belonging to hotel customers.

The steward noted down the various details of the credit cards, which were handed by clients of the hotel for paying their bills. Then, he passed all the details to his computer operator friend who used the details to make online purchases on various websites.

## Chapter 3 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 covers** 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).

### Illustration 1

A school student from Delhi (India), who was regularly teased for having a pockmarked face, used a free hosting provider to create [www.amazing-gents.8m.net](http://www.amazing-gents.8m.net).

He regularly uploaded “morphed” photographs of teachers and girls from his school onto the website. He was arrested when the father of one of the victims reported the case to the police.

### Illustration 2

The CEO of online auction website bazee.com (a part of the ebay group) was arrested by the Delhi police for violating India’s strict laws on cyber pornography.

An engineering student was using the bazee website to sell a video depicting two school students having sexual intercourse. Bazee.com was held liable for distributing porn and hence the CEO was arrested.

### Illustration 3

The CEO of a software company in Pune (India) was arrested for sending highly obscene emails to a former employee.

## Chapter 4 Sale of Illegal Articles

It is becoming increasingly common to find cases where **sale of illegal articles** such as 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. It is practically impossible to control or prevent a criminal from setting up a website to transact in illegal articles.

Additionally, there are several **online payment gateways** that can transfer money around the world at the click of a button. The Internet has also created a marketplace for the sale of unapproved drugs, prescription drugs dispensed without a valid prescription, or products marketed with fraudulent health claims.

Many sites focus on selling prescription drugs and are referred to by some as "**Internet pharmacies.**" These sites offer for sale either approved prescription drug products, or in some cases, unapproved, illegal versions of prescription drugs.

This poses a serious potential threat to the **health and safety of patients.** The broad reach, relative anonymity, and ease of creating new or removing old websites, poses great challenges for law enforcement officials.

### 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.

## Chapter 5 Online Gambling

There are thousands of websites that offer **online gambling**. The special issue with online gambling is that it is legalised in several countries.

So legally the owners of these websites are safe in their home countries. The legal issues arise when a person residing in a **foreign country like India (where such websites are illegal)** gambles on such a website.

### Illustration

The website **ladbrokes.com** permits users to gamble on a variety of sports such as cricket, football, tennis, golf, motor racing, ice hockey, basketball, baseball, darts, snooker, boxing, athletics, rugby, volleyball, motor cycling etc.

Additionally it also features an online casino. The website has no technical measures in place to prohibit residents of certain countries (where online gambling is illegal) from betting at their website.

## Chapter 6 Intellectual Property Crimes

These include software piracy, copyright infringement, trademark violations, theft of computer source code etc.

### Illustration 1

A software professional from **Bangalore** (India) was booked for stealing the source code of a product being developed by his employers.

He started his own company and allegedly used the stolen source code to launch a new software product.

### Illustration 2

In 2003, a computer user in **China** obtained the source code of a popular **game** Lineagell from an unprotected website.

This proprietary code was then sold to several people in 2004.

One of those people set up a website, [www.l2extreme.com](http://www.l2extreme.com), to offer the "Lineage" game at a discount.

Despite legal warnings from the South Korean company that owned the Lineage source code, the suspect did not shut down the site. He rented powerful servers - enough to accommodate 4,000 simultaneous gamers - and solicited donations from users to help defray the costs.

The loss in potential revenues for the South Korean company was estimated at \$750,000 a month. The US FBI arrested the suspect and the website was shut down.

## Chapter 7 Email Spoofing

A **spoofed email** is one that appears to originate from one source but actually has been sent from another source e.g Pooja has an e-mail address pooja@asianlaws.org.

Her ex-boyfriend, Sameer spoofs her e-mail and sends obscene messages to all her acquaintances. Since the e-mails appear to have originated from Pooja, her friends may take offence and relationships may be spoiled for life.

### Illustration 1

In an American case, a teenager made millions of dollars by spreading false information about certain companies whose shares he had short sold.

This misinformation was spread by sending spoofed emails, purportedly from news agencies like Reuters, to share brokers and investors who were informed that the companies were doing very badly.

Even after the truth came out the values of the shares did not go back to the earlier levels and thousands of investors lost a lot of money.

### Illustration 2

A branch of the erstwhile Global Trust Bank in India experienced a run on the bank. Numerous customers decided to withdraw all their money and close their accounts.

An investigation 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.

The spoofed email appeared to have originated from the bank itself.

## Chapter 8 Forgery

Counterfeit currency notes, postage and revenue stamps, mark sheets, academic certificates etc are made by criminals using **sophisticated computers, printers and scanners**.

### Illustration 1

In October 1995, Economic Offences Wing of Crime Branch, Mumbai (India), seized over 22,000 counterfeit share certificates of eight reputed companies worth Rs. 34.47 crores.

These were allegedly prepared using Desk Top Publishing Systems.

### Illustration 2

Abdul Kareem Telgi, along with several others, was convicted in India on several counts of counterfeiting stamp papers and postage stamps totalling several billion rupees.

## Chapter 9 Cyber Defamation

This occurs when defamation takes place with the **help of computers and / or the Internet**. e.g. Sameer publishes defamatory matter about Pooja on a website or sends e-mails containing defamatory information to Pooja's friends.

### Illustration 1

Abhishek, a teenaged student was arrested by the Thane police in India following a girl's complaint about tarnishing her image in the social networking site Orkut.

Abhishek had allegedly created a fake account in the name of the girl with her mobile number posted on the profile. The profile had been sketched in such a way that it drew lewd comments from many who visited her profile.

The Thane Cyber Cell tracked down Abhishek from the false e-mail id that he had created to open up the account.

### Illustration 2

The Aurangabad bench of the Bombay high court issued a notice to Google.com following a public interest litigation initiated by a young lawyer.

The lawyer took exception to a community called 'We hate India', owned by someone who identified himself as Miroslav Stankovic.

The community featured a picture of the Indian flag being burnt.

### Illustration 3

Unidentified persons posted obscene photographs and contact details of a Delhi school girl. Suggestive names like 'sex teacher' were posted on the profile. The matter came to light after the girl's family started receiving vulgar calls referring to Orkut.

## Chapter 10 Cyber Stalking

**Cyber stalking** refers to the use of the Internet, e-mail, or other electronic communications devices to stalk another person.

Stalking generally involves harassing or threatening behaviour that an individual engages in repeatedly, such as following a person, appearing at a person's home or place of business, making harassing phone calls, leaving written messages or objects, or vandalizing a person's property.

Most stalking laws require that the perpetrator make a credible threat of violence against the victim; others include threats against the victim's immediate family.

### Illustration 1

In the first successful prosecution under the California (USA) cyber stalking law, prosecutors obtained a guilty plea from a 50-year-old former security guard who used the Internet to solicit the rape of a woman who rejected his romantic advances.

He terrorized the 28-year-old victim by impersonating her in various Internet chat rooms and online bulletin boards, where he posted, along with her telephone number and address, messages that she fantasized about being raped. On at least six occasions, sometimes in the middle of the night, men knocked on the woman's door saying they wanted to rape her.

### Illustration 2

An honours graduate from the University of San Diego in USA terrorized five female university students over the Internet for more than a year. The victims received hundreds of violent and threatening e-mails, sometimes receiving four or five messages a day. The student, who pleaded guilty, told the police that he had committed the crimes because he thought the women were laughing at him and causing others to ridicule him.

In reality, the victims had never met him.

## Chapter 11 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. For example, there are online contests in which hackers are awarded points for defacing the largest number of web sites in a specified amount of time.

Corporations are also targeted more often than other sites on the Internet and they often seek to take measures to protect themselves from defacement or hacking in general.

Web sites represent the image of a company or organisation and these are therefore especially vulnerable to defacement. Visitors may lose faith in sites that cannot promise security and will become wary of performing online transactions.

After defacement, sites have to be shut down for repairs, sometimes for an extended period of time, causing expenses and loss of profit.

### Illustration 1

Mahesh Mhatre and Anand Khare (alias Dr Neukar) were arrested in 2002 for allegedly defacing the website of the Mumbai Cyber Crime Cell. They had allegedly used password cracking software to crack the FTP password for the police website.

They then replaced the homepage of the website with pornographic content. The duo was also charged with credit card fraud for using 225 credit card numbers, mostly belonging to American citizens.

## Chapter 12 Email Bombing

**Email bombing** refers to sending a large number of emails to the victim resulting in the victim's email account (in case of an individual) or mail servers (in case of a company or an email service provider) crashing.

Email bombing is a **type of denial-of-service attack**. A denial-of-service attack is one in which a flood of information requests is sent to a server, bringing the system to its knees and making the server difficult to access.

### Illustration 1

A British teenager was cleared of launching a denial-of-service attack against his former employer, in a ruling under the UK Computer Misuse Act.

The teenager was accused of sending 5 million e-mail messages to his ex-employer that caused the company's e-mail server to crash.

The judge held that the UK Computer Misuse Act does not specifically include a denial-of-service attack as a criminal offence.

### Illustration 2

In one case, a foreigner who had been residing in Simla (India) for almost 30 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.

## Chapter 13 Data Diddling

One of the most **common forms of computer crime is data diddling** - illegal or unauthorized data alteration. These changes can occur before and during data input or before output.

Data diddling cases have affected banks, payrolls, inventory records, credit records, school transcripts and virtually all other forms of data processing known.

### Illustration 1

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 New Delhi Municipal Council.

Collection of money, computerized accounting, record maintenance and remittance in the 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.

### Illustration 2

A keyboard operator processing orders at an Oakland USA department store changed some delivery addresses and diverted several thousand dollars worth of store goods into the hands of accomplices.

### Illustration 3

A ticket clerk at the Arizona Veterans' Memorial Coliseum in USA issued full-price basketball tickets, sold them and then, tapping out codes on her computer keyboard, recorded the transactions as half-price sales.

## Chapter 14 Salami Attacks

These attacks are used for committing **financial crimes**. The key here is to make the alteration so insignificant that in a single case it would go completely unnoticed.

For instance, a bank employee inserts a program, into the bank's servers, that deducts a small amount of money (say Rs. 2 a month) from the account of every customer.

No account holder will probably notice this unauthorized debit, but the bank employee will make a sizeable amount of money every month.

The attack is called “**salami attack**” as it is analogous to slicing the data thinly, like a salami.

### Illustration 1

Four executives of a rental-car franchise in Florida USA defrauded at least 47,000 customers using a salami technique. They modified a computer billing program to add five extra gallons to the actual gas tank capacity of their vehicles.

From 1988 through 1991, every customer who returned a car without topping it off ended up paying inflated rates for an inflated total of gasoline. The thefts ranged from \$2 to \$15 per customer difficult for the victims to detect.

### Illustration 2

In January 1997, Willis Robinson of Maryland USA, was sentenced to 10 years in prison for “having reprogrammed his Taco Bell driveup - window cash register - causing it to ring up each \$2.99 item internally as a 1-cent item, so that he could pocket \$2.98 each time”.

The management assumed the error was hardware or software and only caught the perpetrator when he bragged about his crime to coworkers.

## Chapter 15 Denial of Service Attacks

**Denial of Service Attacks** (DOS Attacks) involve flooding a computer with more requests than it can handle. This causes the computer (e.g. a web server) to crash and results in authorized users being unable to access the service offered by the computer.

Another variation to a typical denial of service attack is known as a **Distributed Denial of Service (DDoS)** attack wherein the perpetrators are many and are geographically widespread.

### Illustration 1

A series of distributed denial of service attacks in February 2000 crippled many popular websites including yahoo.com, amazon.com and cnn.com

### Illustration 2

A series of more than 125 separate but coordinated denial of service attacks hit the cyber infrastructure of Estonia in early 2007.

The attacks were apparently connected with protests against the Estonian government's decision to remove a Soviet-era war memorial from the capital city.

It is suspected that the attacks were carried out by Russian hackers. The attack lasted several days.

## Chapter 16 Virus / Worm Attacks

**Computer viruses** are small software programs that are designed to spread from one computer to another and to interfere with computer operation.

A **virus** might corrupt or delete data on the victim's computer, use the victim's e-mail program to spread itself to other computers, or even erase everything on the victim's hard disk.

Viruses are most easily spread by attachments in e-mail messages or instant messaging messages. Viruses can be disguised as attachments of funny images, greeting cards, or audio and video files. Viruses can also spread through downloads on the Internet. They can be hidden in illicit software or other files or programs.

**Worms**, unlike viruses do not need the host to attach themselves to. They merely make functional copies of themselves and do this repeatedly till they eat up all the available space on a computer's memory.

**Brain** (in its first incarnation written in January 1986) is considered to be the first computer virus for the PC. The virus is also known as Lahore, Pakistani, Pakistani Brain, Brain-A and UIUC.

The virus was written by two brothers, Basit and Amjad Farooq Alvi, who lived in **Lahore, Pakistan**. The brothers told TIME magazine they had written it to protect their medical software from piracy and was supposed to target copyright infringers only.

The virus came complete with the brothers' address and three phone numbers, and a message that told the user that their machine was infected and for inoculation the user should call them.

When the brothers began to receive a large number of phone calls from people in USA, Britain, and elsewhere, demanding them to disinfect their machines, the brothers were stunned and tried to explain to the outraged callers that their motivation had not been malicious.

They ended up having to get their phone lines cut off and regretted that they had revealed their contact details in the first place. The brothers are still in business in Pakistan as internet service providers in their company called **Brain Limited**.

### Illustration 1

The VBS\_LOVELETTER virus (better known as the Love Bug or the ILOVEYOU virus) was reportedly written by a Filipino undergraduate.

In May 2000, this deadly virus became the world's most prevalent virus. Losses incurred during this virus attack were pegged at US \$ 10 billion.

VBS\_LOVELETTER utilized the addresses in Microsoft Outlook and e-mailed itself to those addresses. The e-mail, which was sent out, had "ILOVEYOU" in its subject line.

The attachment file was named "LOVELETTER- FOR-YOU.TXT.vbs". People wary of opening e-mail attachments were conquered by the subject line and those who had some knowledge of viruses, did not notice the tiny .vbs extension and believed the file to be a text file.

The message in the e-mail was "kindly check the attached LOVELETTER coming from me".

### Illustration 2

Probably the world's most famous worm was the Internet worm let loose on the Internet by Robert Morris sometime in 1988.

The Internet was, then, still in its developing years and this worm, which affected thousands of computers, almost brought its development to a complete halt.

It took a team of experts almost three days to get rid of the worm and in the meantime many of the computers had to be disconnected from the network.

## Chapter 17 Trojans and Keyloggers

A **Trojan**, as this program is aptly called, is an unauthorized program which functions from inside what seems to be an authorized program, thereby concealing what it is actually doing.

**Keyloggers** are regularly used to log all the strokes a victim makes on the keyboard. This assumes sinister proportions, if a key logger is installed on a computer which is regularly used for online banking and other financial transactions.

Key-loggers are most commonly found in public computers such as those in cyber cafes, hotels etc.

### Illustration 1

A young lady reporter was working on an article about online relationships. The article focused on how people can easily find friendship and even love on the Internet. During the course of her research she made a lot of online friends. One of these 'friends' managed to infect her computer with a Trojan.

This young lady stayed in a small one bedroom apartment and her computer was located in one corner of her bedroom. Unknown to her, the Trojan would activate her web camera and microphone even when the Internet was switched off. A year later she realized that hundreds of her pictures were posted on pornographic sites around the world!

### Illustration 2

The network administrator in a global bank received a beautifully packed CD ROM containing "security updates" from the company that developed the operating system that ran his bank's servers. He installed the "updates" which in reality was Trojanized software. 3 years later, the effects were still being felt in the bank's system!

## Chapter 18 Internet Time Theft

This connotes the usage by an unauthorized person of the Internet hours paid for by another person.

### Illustration

In May 2000, the Delhi police arrested an engineer who had misused the login name and password of a customer whose Internet connection he had set up.

The case was filed under the Indian Penal Code and the Indian Telegraph Act.

## Chapter 19 Web Jacking

Just as **conventional hijacking** of an airplane is done by using force, similarly web jacking means forcefully taking over control of a website. The motive is usually the same as hijacking – ransom.

The perpetrators have either a monetary or political purpose which they try to satiate by holding the owners of the website to ransom.

This occurs when someone forcefully takes control of a website (by cracking the password and later changing it). The actual owner of the website does not have any more control over what appears on that website.

### How does web jacking take place?

The administrator of any website has a **password and a username** that only he (or someone authorized by him) may use to upload files from his computer on the web server (simply put, a server is a powerful computer) where his website is hosted.

Ideally, this password remains **secret** with the administrator. If a hacker gets hold of this username and password, then he can pretend to be the administrator. Computers don't recognize people – only usernames and passwords.

The web server will grant control of the website to whoever enters the correct password and username combination.

There are many ways in which a **hacker may get to know a password**, the most common being password cracking wherein a “**cracking software**” is used to guess a password.

**Password cracking attacks** are most commonly of two types. The first one is known as the **dictionary attack**. In this type of attack the software will attempt all the words contained in a predefined dictionary of words.

**For example**, it may try Rahim, Rahul, Rakesh, Ram, Reema, Reena ... in a predefined dictionary of Indian names. These types of dictionaries are readily available on the Internet.

The other form of password cracking is by using **brute force**. In this kind of attack the software tries to guess the password by trying out all possible combinations of numbers, symbols, letters till the correct password is found.

**For example**, it may try out password combinations like abc123, acbd5679, sdj#%^, weuf\*(-)\*.

Some software, available for password cracking using the brute force technique, can check a huge number of password combinations per second.

When compared with a dictionary attack, a brute force attack takes more time, but it is definitely more successful.

### Illustration

In an incident reported in the USA, the owner of a hobby website for children received an e-mail informing her that a group of hackers had gained control over her website.

They demanded a ransom of 1 million dollars from her. The owner, a schoolteacher, did not take the threat seriously. She felt that it was just a scare tactic and ignored the e-mail.

The hackers web jacked her website and subsequently altered a portion of the website which was entitled 'How to have fun with goldfish'.

In all the places where it had been mentioned, they had replaced the word 'goldfish' with the word 'piranhas'. Piranhas are tiny but extremely dangerous flesh-eating fish. Many children had visited the popular website and had believed what the contents of the website suggested. These unfortunate children followed the instructions, tried to play with piranhas, which they bought from pet shops, and were very seriously injured!

## Chapter 20 Email Frauds

*Dear Mr. Justin Williams, I'm Vikas Manjit Singh from Punjab (India). I belong to a city named Ludhiana.*

*Mr. Williams, I am having a brother in Canada who is also named Justin Williams. He was adopted from my parents by some Mr. William Ram of Welland. Me and my mum came over to Canada to leave Justin to his new family (William Ram's Family). It happened in June 1985.*

*So Mr. Justin Williams, if you are the same person I'm talking about. Then please give me some time so that I can let you know the realities.*

---

Imagine the thoughts going through Mr. Justin William's head after reading this email. Is he really adopted? Where are his birth parents? Is this email from his birth brother?

In reality, this is a **scam email** originating from a college in Sangroor (India)! Canadian citizens are targeted with these emails. If the targets start believing the sender to be their brother, they are asked to send money so that their "brother" can travel to Canada with the proof of the victim's adoption!

This is just one of the hundreds of email scams being perpetrated on the Internet. These scams are commonly referred to as **Nigerian 419 scams**. These scam emails are believed to originate from Nigeria and section 419 of the Nigerian Penal Code relates to cheating (**like the famous section 420 of the Indian Penal Code**).

The **419 letter scams** originated in the early 1980s as the oil-based economy of Nigeria went downhill. In the 1990s, letter scams gave way to email scams.

In 2007, **Asian School of Cyber Laws** conducted a 3 month intensive investigation of hundreds of scam emails. The results were very surprising to say the least. Less than 10% of these emails had actually originated from Nigeria!

A majority of these emails (more than 60%) have originated from Israel, followed by the Netherlands, UK and other European countries. The “birth brother” email was the only one originating from India.

Most of these scam emails promise the receiver millions (or sometimes billions) of dollars. Most commonly the email says that some rich African bureaucrat or businessman or politician has died and left behind a lot of money.

The scamster states that the Government is going to confiscate the money. The only way out is to transfer the money to the bank account of the email recipient. All that the email recipient has to do is send his bank account details. For this a generous fee of a few million dollars will be paid!

If someone actually falls for this scam and provides the bank details, he is sent some official looking documents relating to the bank transfer of a huge sum of money. Once the victim is convinced of the “genuineness” of the transaction, something appears to go wrong.

The victim is informed that a small amount of money (ranging from US\$ 100 to 2500) is needed for bank charges or other paper work. This money is the motive behind the elaborate scam. Once the victim pays this money, the scamster disappears from the scene.

The **lottery scam emails** inform the recipient that he has won a million dollar lottery run by Microsoft, Yahoo or some other well known global company. The winner is asked to provide his bank details and pay a small sum for bank charges and other processing fees.

Another scam email begins with “**This is to inform you that we are in possession of a consignment, deposited by British National Lottery which is to be couriered to you**”.

The email asks for 470 pounds to be sent to the courier company so that the cheque for the lottery prize can be sent.

Another scam email comes with the subject line “**Blessed is the hand that giveth**”.

The sender claims to be a widow on her deathbed. She wants to donate her wealth to someone who will pray for her.

Another scam email comes from an “**employee of the Euro Lottery**”.

The “employee” claims to be in a position to carry out a lottery fraud and is willing to share the money with the email recipient.

What is **common** in all these scams is that scanned versions of official documents are emailed to potential victims.

Once the victim is convinced of the genuineness of the transaction, a small fee is requested for meeting bank charges / legal fees / courier charges etc. It is this small fee that is the motive behind the scam.

It is believed that thousands of people are defrauded of billions of dollars every year through these scams.

### Illustration

In 2005, an Indian businessman received an email from the Vice President of a major African bank offering him a lucrative contract in return for a kickback of Rs 1 million.

The businessman had many telephonic conversations with the sender of the email. He also verified the email address of the ‘Vice President’ from the website of the bank and subsequently transferred the money to the bank account mentioned in the email.

It later turned out that the email was a spoofed one and was actually sent by an Indian based in Nigeria.

## Chapter 21 Cyber Terrorism

Computer crime has hit mankind with unbelievable severity. Computer viruses, worms, trojans, denial of service attacks, spoofing attacks and e-frauds have taken the real and virtual worlds by storm. However, all these are pale in the face of the most dreaded threat – that of **cyber terrorism**.

**Asian School of Cyber Laws** has defined cyber terrorism as:

***"Cyber terrorism is the premeditated use of disruptive activities, or the threat thereof, in cyber space, with the intention to further social, ideological, religious, political or similar objectives, or to intimidate any person in furtherance of such objectives".***

### Illustration 1

In 1996, a computer hacker allegedly associated with the White Supremacist movement temporarily disabled a US based Internet Service Provider (ISP) and damaged part of its record keeping system. The ISP had attempted to stop the hacker from sending out worldwide racist messages under the ISP's name. The hacker signed off with the threat, "you have yet to see true electronic terrorism. This is a promise."

### Illustration 2

In 1998, Spanish protestors bombarded the Institute for Global Communications (IGC) with thousands of bogus e-mail messages. Email was tied up and undeliverable to the ISP's users, and support lines were tied up with people who couldn't get their mail. The protestors also spammed IGC staff and member accounts, clogged their Web page with bogus credit card orders, and threatened to employ the same tactics against organizations using IGC services.

They demanded that IGC stop hosting the website for the Euskal Herria Journal, a New York-based publication supporting Basque independence. Protestors said IGC supported terrorism because a section on the web pages contained materials on the terrorist group ETA, which claimed responsibility for assassinations of Spanish political and security officials, and attacks on military installations. IGC finally relented and pulled the site because of the "mail bombings."

## Chapter 22 Use of Encryption by Terrorists

A disturbing trend that is emerging nowadays is the increasing use of encryption, high-frequency encrypted voice/data links, encryption software like Pretty Good Privacy (PGP) etc by terrorists and members of organized crime cartels.

**Strong encryption** is the criminal's best friend and the policeman's worst enemy.

### Illustration 1

Leary, who was sentenced to 94 years in prison for setting off fire bombs in the New York (USA) subway system in 1995, had developed his own algorithm for encrypting the files on his computer.

### Illustration 2

The Cali cartel is reputed to be using sophisticated encryption to conceal their telephone communications, radios that distort voices, video phones which provide visual authentication of the caller's identity, and instruments for scrambling transmissions from computer modems.

### Illustration 3

On March 20, 1995, the Aum Supreme Truth cult dropped bags of sarin nerve gas in the Tokyo subway, killing 12 people and injuring 6,000 more. Members of the cult had developed many chemical and biological weapons, including Sarin, VX, Mustard gas, Cyanide, botulism, anthrax and Q fever.

It is believed that preparations were underway to develop nuclear capability. The cult was also believed to be developing a "death ray" that could destroy all life! The records of the cult had been stored in encrypted form (using the RSA algorithm) on computers. The enforcement authorities were able to decrypt the information as the relevant private key was found in a floppy disk seized from the cult's premises. The encrypted information related to plans of the cult to cause mass deaths in Japan and USA.

**Data64 Techno Solutions Pvt. Ltd. is an innovative educational organisation that provides cutting edge courses in the field of Information Technology with specific focus on cyber crime investigation and cyber security.**

**Courses offered by Data64 Techno Solutions:**

- 1. Web Hacking & Security Professional**
- 2. Cyber Forensics Professional**
- 3. Information Technology Law**

**At Data64, we aim to revolutionize the way education is delivered.**

The logo for Data64 consists of the word "data" in a blue, lowercase, sans-serif font, followed by the number "64" in a larger, red, lowercase, sans-serif font.

**Techno Solutions Pvt. Ltd.**

(Incubated by Science & Technology Park)

An Initiative of Department of Science & Technology,  
Government of India

---

**Admissions Office  
1st Floor, Sigma House,  
Senapati Bapat Road, Pune - 411016**

---

**+91-20-6400 0000, +91-20-6400 6464**