CYBERCRIME AWARENESS HANDBOOK FOR POLICE OFFICERS

(3-DAYS PROGRAM)

सत्यमेव जयते

Ministry of Home affairs

Contents

Document Control

Document Information:

Owner	Ministry of Home Affairs
Document Status	Approved
Date Effective	12 November 2018

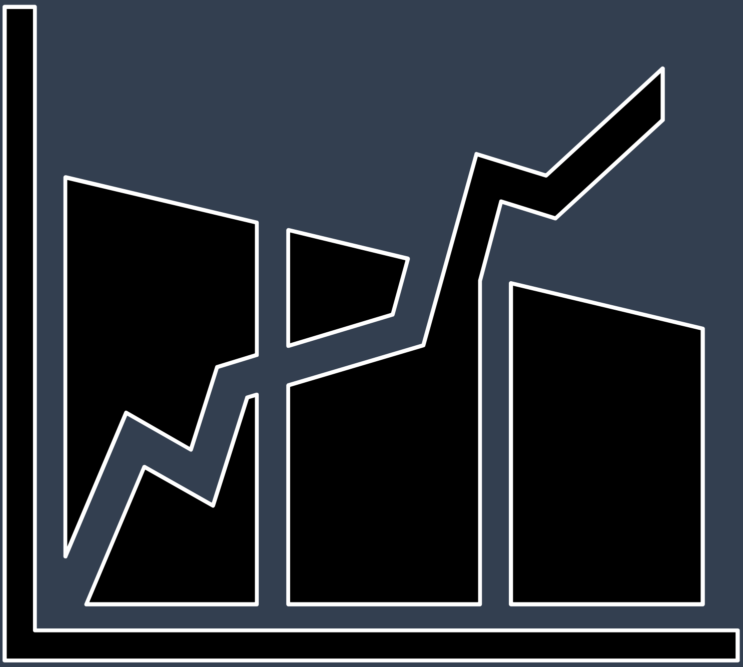
Document Revision History

Version No.	Status	Date	Author	Reviewed by	Approved by	Change Log
1.0	Final	12 November 2018	PMU	Advisor(ICT),MHA	JS,CIS,MHA	Version 1

Acknowledgement

The Ministry of Home Affairs (MHA) would like to thank the central training institutes, stakeholder Ministries, States, academia and professional bodies for recommending course structure for the program and state Law Enforcement Agencies for providing inputs and feedback for this book which is created, compiled and edited by CCPWC - PMU team MHA

As per the Advisory released by MHA on 2/2/18 (F.No 22006/2/2017-CIS-II), a recommended training schedule is given under Annexure 4



CHAPTER-I

Emerging Threat Landscape in cyber crimes

CHAPTER-I: Emerging Threat Landscape in cyber crimes

Why Should I read this Chapter?

After reading this chapter, you would be able to:

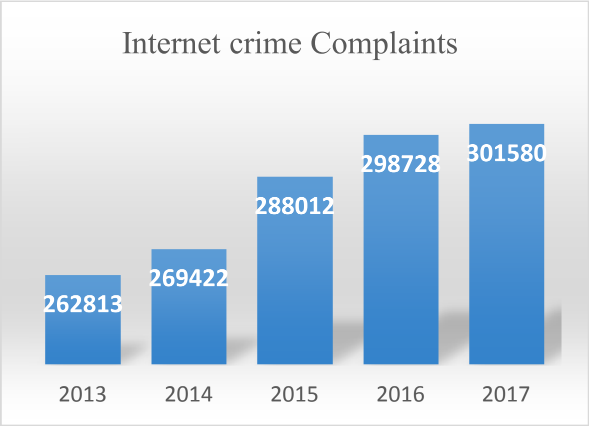
- Understand Emerging Threat Land Scape in Cyber Crimes
- Understand about the various Cyber Crimes which could have potential impact on an individual or on an organisation.
- Identify ways through which Cybercrime could be carried out

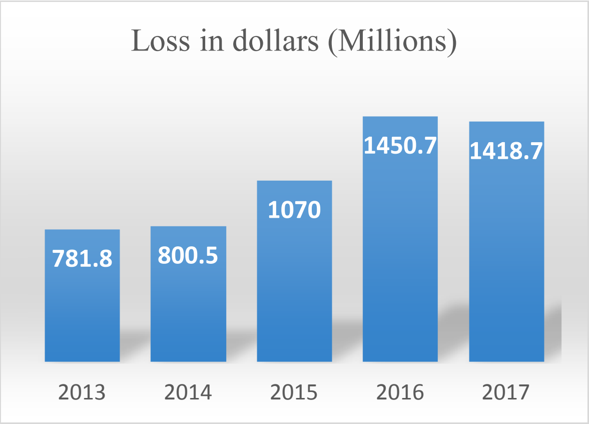
Computers and internet have transformed the shape of our lives. They are being used by individuals and societies to make their life easier. The popularity of Internet has a dark side, as it has evolved from a friendly research network to a hotbed of criminal activity such as identity theft, card frauds, distribution of child sexual abuse materials, data theft etc.,

1.1. Statistics on Cyber Crimes

Internet Crime Complaint Centre Statistics (IC3)

In May 2000, the Internet Crime Complaint Centre (IC3) was established as a centre to receive complaints of Internet crime. There have been 4,063,933 complaints reported to the IC3 since its inception. The mission of the IC3 is to provide the public with a reliable and convenient reporting mechanism to submit information to the FBI concerning suspected Internet-facilitated criminal activity, and to develop effective alliances with industry partners. Information is analysed and disseminated for investigative and intelligence purposes, for law enforcement, and for public awareness.

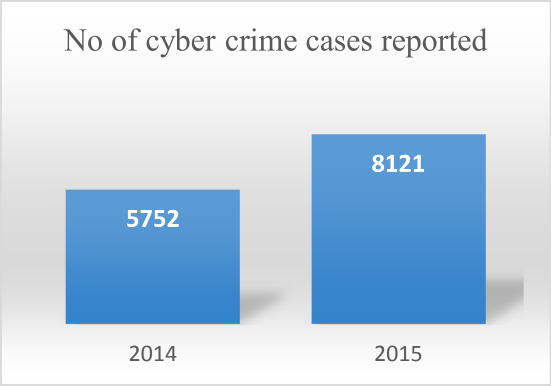




*Over the last five years, the IC3 has received an average of more than 284,000 complaints per year.

*Over the years 2013 to 2017, IC3 received a total of 1,420,555 complaints, and a total reported loss of $5.52 billion.

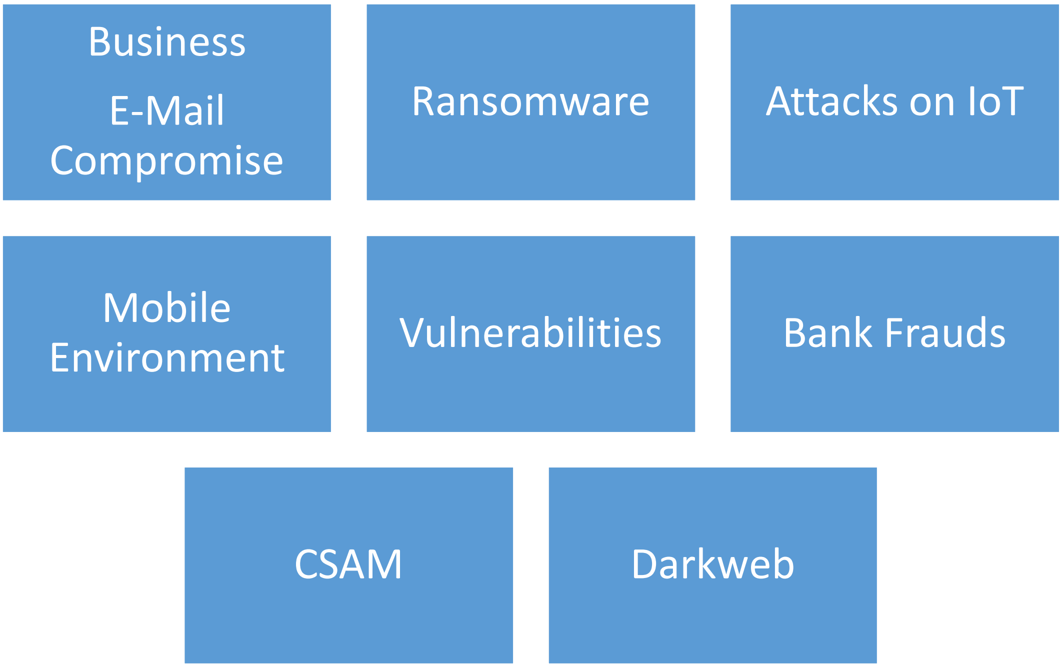
National Crime Records Bureau (NCRB) Statistics



The statistical data covered in the NCRB report have been obtained from States/UTs Police.

The number of cases reported under Cyber Crimes (State, UT & City-wise) increased by 41.2% in 2015 over 2014.

1.2. Emerging Cybercrime trends



Business E-Mail Compromise

Ransomware

Attacks on IoT

Mobile Environment

Vulnerabilities

Bank Frauds

CSAM

Darkweb

1.3. Business E-Mail Compromise

Business e-mail compromise (BEC) is a sophisticated scam targeting businesses that often work with foreign suppliers and/or businesses and regularly perform online money transfers. The Email Account Compromise (EAC) is the variation of BEC that targets individuals who regularly perform online transactions with foreign entities/companies. It should be noted while most BEC and EAC victims reported using wire transfers as their regular method of transferring business funds. Both scams typically involve one or more fraudsters, who compromise legitimate business email accounts through social engineering or computer intrusion techniques to conduct unauthorized transfers of funds.

1.4. Ransomware

Among the different malware variants available, ransomware or cryptoware, to be more precise has become the dominant threat. While more 'commercial' data-stealing malware typically still targets desktop Windows users, ransomware is more indiscriminate: its targets range from individual users' devices to large organisations and even governments.

1.5. Attacks on IoT

Internet of Things (IoT) is an ecosystem of connected physical objects that are accessible through the internet. The ‘thing’ in IoT could be a person with a heart monitor or an automobile with built-in-sensors, i.e. objects that have been assigned an IP address and have the ability to collect and transfer data over a network without manual assistance or intervention. Some of the researchers are also looking future of the world in this technology. Since then significant research and development have taken place on IoT.

Much of the IoT communication comes from computing devices and embedded sensor Systems used in industrial machine-to-machine (M2M) communication, smart energy grids, home and building automation, vehicle to vehicle communication and wearable computing devices. However, various vulnerabilities are observed which shall keep IoT as a technology in danger. As a result, so many attacks on IoT have been invented before actual commercial implementation of it.
The IoT attack surface is the sum total of all potential security vulnerabilities in devices and associated software and infrastructure in a given network, be it local or the entire Internet.

The Internet of Things (IoT) continues to grow as a prime target for cybercriminals to exploit, according to a new threat report from security firm Symantec. The number of IoT attacks increased from about 6,000 in 2016 to 50,000 in 2017—a 600% rise in just one year, the report found.

The FBI lists the following examples of IoT devices[1]

- Automated devices which remotely or automatically adjust lighting or HVAC
- Security systems, such as security alarms or Wi-Fi cameras, including video monitors used in nursery and day-care settings
- Medical devices, such as wireless heart monitors or insulin dispensers
- Thermostats
- Wearable’s, such as fitness devices
- Lighting modules which activate or deactivate lights
- Smart appliances, such as smart refrigerators and TVs

Any device in that list can be hacked if connected to the Internet and not adequately protected. Furthermore, hacked devices can provide an attacker with access to sensitive data on the same network

[1] FBI Alert Number I-091015-PSA

1.6. Mobile Environment

A decade ago, mobile malware was considered a new and unlikely threat. Many mobile device users even considered themselves immune from such threats.

Today, mobile devices are coming under increasing attack and no one is immune. Some 20 percent of companies surveyed by Dimensional Research for Check Point Software said their mobile devices have been breached. A quarter of respondents didn’t even know whether they’ve experienced an attack. Nearly all (94 percent) expected the frequency of mobile attacks to increase, and 79 percent acknowledged that it’s becoming more difficult to secure mobile devices.

The popular mobile devices include Apple iPhone, Google Android, Research in Motion (RIM) Blackberry, Symbian, and Windows Mobile-based devices.

As far as Mobile Malware distribution is concerned, android based mobile devices are being targeted the most. The reasons being involving but not limited to, leading market share, open source architecture, no formal upgrade process for known vulnerabilities etc.

The malwares distributed through fake/illegitimate apps download websites can perform, including but not limited to, the following actions:

- Take full control over the infected mobile device.
- Send expensive messages and share a user's phone number, email-address, mobile numbers, mobile carrier details as well as GPS Coordinates.
- Record Conversations & send it to the intruder.
- Download more Malwares into the infected device.

1.7. Vulnerabilities

In computer security, vulnerability is a weakness which allows an attacker to reduce a system's information assurance.[2]

A flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's security policy[3]*.*

A criminal can exploit the vulnerabilities and gain unauthorized access to resources .For e.g.: a user opens an email message with attached vulnerable code, which exploits the vulnerable system/application software’s present on the user’s computer to gain unauthorized access to resources on the victims Computer.

1.8. Bank Frauds

With the advances in information technology, most banks in India have migrated to core banking platforms and have moved transactions to payment cards (debit and credit cards) and to electronic channels like ATMs, Internet Banking and Mobile Banking. Fraudsters have also followed customers into this space[4].

Net banking is also called as Internet Banking which refers to the banking services provided by the banks over the internet. ”Various banking services include paying of bills, funds transfer, viewing account statement etc.

[2] www.en.wikipedia.org

[3] IETF RFC 2828

[4] http://www.rbi.org.in/scripts/PublicationReportDetails.aspx?UrlPage=&ID=621

Online transactions are generally accomplished electronic mode of payments like NEFT (National Electronic Funds Transfer) & RTGS (Real Time Gross Settlement). These transactions are generally undertaken remotely, through internet banking, by using specific ID and password provided to the users.

Types of attacks:

1.8.1. Banking Trojans

Trojan is a malicious computer program designed to gain access to confidential information stored or processed through online banking systems.

1.8.2. Man in the browser attack

In order to accomplish MITB attack, the attacker makes use of two weapons-a proxy Trojan and a Vulnerable Web Browser (which is by default installed in the user's Computer).The fraudster achieves the MITB attack by embedding a Proxy Trojan in the user's bowser. The proxy Trojan infects the user's browser exploiting its vulnerabilities. Upon successful exploitation of the user's browser, the Proxy Trojan is able to modify transaction content or conduct operations for the victims in a completely covert fashion.

1.9. Card Frauds

Credit/Debit card frauds involves an unauthorized taking of another's credit card information for the purpose of obtaining goods without paying, or to obtain unauthorized funds from the account

1.9.1. Lost and Stolen Card Fraud

This type of fraud occurs when the card is lost by customer and lands up in the hands of a fraudster or the card is stolen by fraudster and subsequently misused.

1.9.2. Counterfeit Card Fraud or Skimming

- A counterfeit card can be a fake card or a valid one that's been altered or recoded.
- Most cases involve skimming, when the data on a user's card's magnetic strip is electronically copied on to another card without his/her knowledge.
- A Skimmer is a device which is used to capture and store the data from the magnetic stripe of a card
- Skimming commonly occurs at retail outlets – particularly bars, restaurants and petrol stations – and at cash machines that have been illegally fitted with a skimming device. The stolen data is then used to create counterfeit cards.
- Most people are unaware that they've fallen victim to this fraud until their statements arrive.

1.9.3. Card Not Received/Intercepted

This type of fraud occurs when the card is intercepted by fraudster either in connivance with courier boy or using fake ID documents while taking the delivery of card**.**

1.9.4. Mail non-receipt card fraud

This fraud occurs when you order a new card and it's stolen on the way to you. You're at particular risk of this fraud if you live in a property with a communal letterbox, such as a block of flats or a student residence hall.

1.9.5. Set up Companies

In this type of fraud, a residential locality is chosen by the fraudsters to set up their company. A hand written name board is usually seen in this category of fraud. The fraudsters (group) apply for cards across banks using this address as residence cum office, receive the cards, misuse it and flee.

1.10. Child Sexual Abuse Material (CSAM)

Child sexual exploitation refers to the sexual abuse of a person below the age of 18, as well as to the production of images of such abuse and the sharing of those images online.

Online child sexual exploitation is a constantly evolving phenomenon and is shaped by developments in technology. Mobile connectivity, growing internet coverage in developing countries

Peer-to-peer (P2P) networks and anonymised access like Darknet networks (e.g. Tor). These computer environments remain the main platform to access child abuse material and the principal means for non-commercial distribution. These are invariably attractive for offenders and easy to use. Pay-as-you-go streaming solutions, which provide a high degree of anonymity to the viewer, are furthering the trend in the commercial live-streaming of child sexual abuse.

1.11. Types of Cybercrimes

The methods and technologies cybercriminals use to commit their crimes are innumerable and continue to grow each year in both number and sophistication. Listed below are few common types of cybercrimes.

1.11.1. Email related crime

The ease, speed and relative anonymity of email have made it a powerful tool for misuse by cyber criminals. Some of the major e-mail related crimes are given below

1.11.2. Email spoofing

Email spoofing is the forgery of an email header so that the message appears to have originated from someone or somewhere other than the actual source. Email spoofing is an approach used in phishing and spam campaigns because people are more likely to open an email when they think it has been sent by a legitimate source. There are different types of email spoofs, but they all have similarities. One main similarity is that you receive an email which claims to be from someone you know but in reality, it has been sent by another source.

1.11.3. Phishing/vishing

Phishing involves fraudulently acquiring (very often attacker try to disguise themselves and their communication as genuine) the sensitive information (e.g. online banking passwords, credit card details, debit card details etc.). The suspect's identity might be traced using the IP addresses of the suspected email sent.

If you click on a link in an email spoof, it might direct you to a fake webpage to collect your sensitive information.

Note: Always check the link before clicking. Hover over it to preview the URL, and look carefully for misspelling or other irregularities.

1.11.4. Email bombing

Email bombing is a form of an abuse consisting of sending huge volumes of email to a single address or recipient in an attempt to overflow the mailbox or overwhelm the server where the email address is hosted causing denial of service.

1.11.5. Spamming

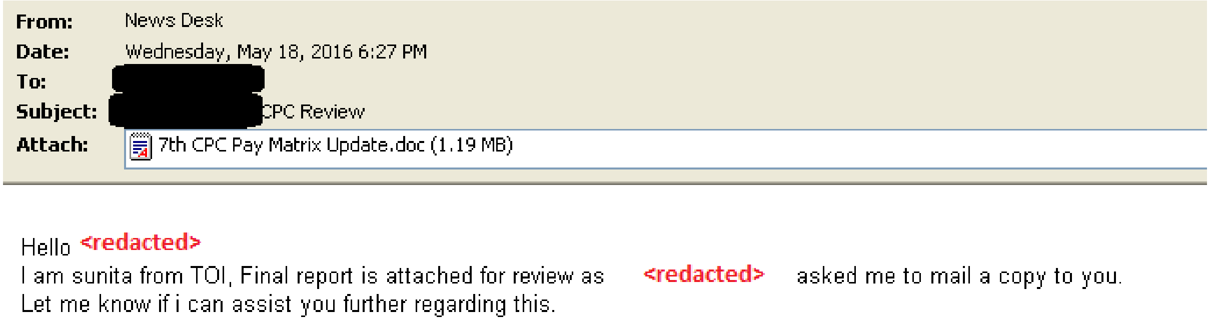
Spamming is sending an unsolicited message, especially to promote a product or services, as well as sending messages repeatedly through a communication medium. Spammers not only use e-mail services but also use other channels such as SMS, TV advertising, social networking, Internet forums, Blogs etc.

1.11.6. Spear phishing

is a directed attack which is one of the very rampant email frauds till date. Spear phishing is a targeted phishing aimed at specific individuals or groups within an organization especially corporates. Spear phishing makes the use of information about a target to make attacks more specific and personal to the target. Spear-phishing emails, for instance, may refer to their targets by their specific name, rank, designation or position instead of using generic titles as in normal phishing campaigns.

Spear-phishing emails can have attachments of varying file types e.g. XLS, PDF, DOC, .DOCX etc. The malware then accesses a malicious command-and-control (C&C) server to take instructions from a remote user. At the same time, to hide malicious events malware usually drops a decoy document that will open when the malware or exploit runs.

For example, cyber criminals sent an MS word attachment titled ‘7th Central Pay Commission’, knowing the high interest among government employees. These emails were generated over a fake domain timesofindiaa (note the extra letter ‘a’ in the end).



From: News Desk
Date: Wednesday, May 18, 2016 6:27 PM
To: [redacted]
Subject: [redacted]CPC Review
Attach: 7th CPC Pay Matrix Update.doc (1.19 MB)

Hello <redacted>
I am sunita from TOI, Final report is attached for review as <redacted> asked me to mail a copy to you.
Let me know if i can assist you further regarding this.

Source: Fire eye blog

1.11.7. Illegal Online transaction

Through illegal online transactions the perpetrator deprives the victim for funds, personal property, interest or sensitive information via the Internet. There are majorly three types of frauds:

- fraudulent or unauthorized transactions
- Lost or stolen merchandise
- False requests for a refund, return or bounced cheques

Fraudsters have become savvy at illegally obtaining information online. Cyber criminals often pose as a legitimate representative and contact credit/Debit card owners asking for sensitive information. They may use one or more of the following means of interaction to steal personal data:

- Email
- Texting malware on smartphones
- Instant messaging
- Rerouting traffic to fraudulent websites
- Phone calls

1.11.8. Job Frauds

It involves deceiving people seeking employment by giving them the false hope of earning high salaries or extra income. There are numerous methods where scammers come up with attractive offers such as easy hire, easy work, high wages, flexible working hours etc.,

1.11.9. Cyber defamation

As per Indian Penal Code (IPC) whoever, by words either spoken or intended to be read, or by signs or by visible representations, makes or publishes any imputation concerning any person intending to harm, or knowing or having reason to believe that such imputation will harm, the reputation of such person, is said to defame that person. Cyber defamation is the new form of committing traditional defamation where virtual communication is used to defame an individual or organization.

1.11.10. Ponzi scheme

A Ponzi scheme is a fraudulent investment scam where criminals lure the victims promising high rates of return with little risk.

e.g. Money Trade Coin (MTC) - A crypto currency scam estimated to be in the range of Rs 300 crore to Rs 500 crore.

1.12.11. Cyber stalking

Cyber stalking is a criminal practice in which attacker use internet and other electronic devices to persistently harass victims.

e.g. State of Maharashtra Vs Atul Ganesh Patil

A women had come for job interview to a company and wrote her mobile number in the entry register. The guard saved her contact details and started sending multiple obscene WhatsApp messages and even called her repeatedly to talk obscene things thereby committing crime of stalking her. In this case, victim blocked his number. However, the guard started sending her obscene messages from his friend’s mobile phone. A case was registered under IPC 354D. The police acted swiftly completing the investigation and prepared a charge sheet within 24 hours.

1.11.11. Cyber bullying

It is a form of offense committed by using virtual communication medium like e-mail, social media, SMS, messengers, forums etc., to harass, threaten, embarrass, and humiliate victims. Cyber bullying can be anonymous or it can also have wider audience which can spread quickly. Cyber bullying commonly occurs among teenagers.

1.11.12. Cyber pornography

Cyber pornography is defined as the act of using cyberspace to create, view, distribute, import, or publish pornography or obscene materials.

1.12. Cybercrimes of advanced types

Cybercriminals use various technologies to exploit security holes. These technologies are constantly growing in number and sophistication.

1.12.1. Hacking

It is an attempt to exploit weaknesses for gaining unauthorized access in a computer system or network.

As per IT act, hacking is a term used to describe the act of destroying or deleting or altering any information residing in a computer resource or diminishing its value or utility, or affecting it injuriously in spite of knowing that such action is likely to cause wrongful loss or damage to the object, public or a person.

1.12.2. Virus

Computer Virus means any computer instruction, information, data or programme that destroys, damages degrades or adversely affects the performance of a computer resource. It generally attaches itself to another computer resource and operates when a programme, data or instruction is executed or some other event takes place in that computer resource.

1.12.3. Worm

It is a self-replicating malicious software that replicates itself to spread across other devices that are connected to a network.

1.12.4. Trojan

It is a malicious software that is camouflaged as a legitimate software e.g. Microsoft office, web browsers, media players, gaming applications etc. However, in reality has a malicious purpose.

1.12.5. Website defacement

It is an attack intended for a Website, which will change the visual appearance of a website and the attacker may post some other indecent, hostile and obscene images, messages, videos, etc., and sometimes make the Website dysfunctional.

The most common cases of website defacement are, hackers of one country try to deface the websites of rival countries to display their technological superiority by infecting with malware.

1.12.6. Salami Attack

An attack is made on a system or network that involves making minor alteration so insignificant that in a single case it would go completely unnoticed. These attacks are generally used for the commission of financial crimes.

1.12.7. Cross-site scripting

Cross-Site Scripting (XSS) is a type of vulnerability in which malicious scripts are injected into content from otherwise trusted websites. The injection occurs when a user clicks on an unsuspected link that is specially designed for attacking a website they are visiting.

Note: Script is a sequence of commands or programs that are written in certain programming languages which may be used to automate certain process on the communication devices like smartphones, laptops, desktops etc.,

1.12.8. Web Jacking

The Web Jacking Attack is an advanced phishing technique where attackers make a clone of a website and send that malicious link to the victim. Once, the victims click the link that looks real he will be redirected to a fake page where attackers try to extract sensitive data such as card numbers, user names, passwords etc., from the victims.

1.12.9. DOS/DDOS attacks

In the Denial of service attack (DoS), an important service offered by a Web site or a server is denied or disrupted thereby causing loss to the intended users of the service. Typically, the loss of service is the inability of a particular network service, such as e-mail, to be available or the temporary loss of all network connectivity and services.

In some cases, DoS attacks have forced the Websites to temporarily cease operation. This often involves sending a large amount of traffic in the form e-mails and other requests to the targeted network or server so that it occupies the entire bandwidth of the system and ultimately results in a crash. The Distributed Denial of Service (DDoS) is a type of attack in which multiple systems are used to flood the bandwidth of the targeted system.

1.13. Dark Web

The deep web is part of the internet where a typical search engine cannot index. The dark web/ darknets is a subset of deep web that is intentionally made hidden through overlay networks and require specific software, configurations or authorization to access.

Frauds are openly discussed on the underground forums of the Dark Web where illicit vendors offer fraudulent services. These services include but not limited to, launching a DoS attack on websites, the sale of malware, illegal drugs, weapons, cyber espionage on behalf of clients and the list goes on. Most of the vendors accept the payment through crypto-currencies and specially Bitcoins due to its popularity

CHAPTER-II

Introduction to Computers

CHAPTER-II: Introduction to Computers

Why Should I read this Chapter?

After reading this chapter, you would be able to:

- Understand the basic computer fundamental and its components.
- Understand the various computer technologies in perspective of Cybercrime investigation.

2.1. Introduction to Computer Fundamentals

The rapid growth of internet and the technological advancements in the information & communication technologies have transformed the conventional trends and procedures in the investigation of crimes. The law enforcement agencies across the globe are facing challenges with regard to the handling of the crimes involving digital evidences.

The investigation of any criminal case generally starts with gathering the initial information from a variety of sources which includes the evidence present in computers & other digital devices. The Investigating officer needs to have a proper understanding about the characteristics and features of different electronic devices. An attempt is made in this chapter to sensitize the reader about the basics of computers which will help during the investigation of cases involving computers.

Law: "Information" includes data, message, text, images, sound, voice, codes, computer programs, software and databases or micro film or computer generated micro fiche. (***Definition as per ITAA 2008***)

Data: Data is a collection of raw facts from which conclusions may be drawn.

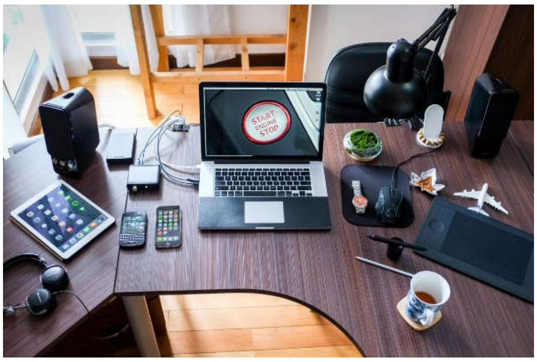
Or

"Data" means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalized manner and is intended to be processed, is being processed or has been processed in a computer system or computer network and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer. (***Definition as per ITAA 2008***)

Information: Information is the intelligence and knowledge derived from data or Information is data arranged in a meaningful way for some perceived purpose.

2.2. What is a Computer?

A **computer** is an electronic device operating under the control of instructions stored in its own memory that can accept data, process the data according to specified rules, produce results and store the results for future use.



A typical computer system is comprised of the following:

Hardware refers to the physical components that make up a computer system. These include the computer's processor, memory, monitor, keyboard, mouse, disk drive, peripherals etc.

Software is any *set of instructions* provided to the computer by the user for performing a specific task.

Some examples of software are web browsers, games, and word processors such as Microsoft Word etc.

Note: "Computer" means any electronic, magnetic, optical or other high-speed data processing device or system which performs logical, arithmetic, and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software, or communication facilities which are connected or related to the computer in a computer system or computer network. (***Definition as per ITAA 2008***)

2.3. Information processing cycle:

A computer converts data into information by performing various actions on the data using both hardware & software. These operations are part of a process called information processing cycle. Each part involves one or more specific components of computer.

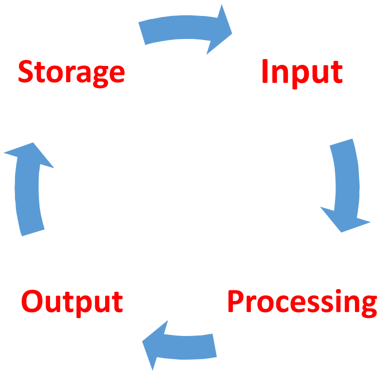


Fig 1: Information Processing Cycle

Input: During this part of the cycle, computer accepts data either from the user or a program for processing. The input device takes the responsibility of converting the data into a suitable form that can be understood by the computer.

Processing: During this part of the cycle, the computers process the data based on instructions obtained from the user or a program.

Output: In this part the computers may be required to display (output) the result of its processing. The processor can output the result or information in a form which is suitable for human understanding. The most widely used output devices are monitor & printer. However, output is an optional step but may be ordered by the user or program.

Storage: The computer stores the result of its processing on a disk or some other kind of storage medium. Storage is also optional in information processing cycle and may not always be required by the user or program.

2.4. Architecture of a computer

A Typical computer system consists of three units:

1. Input device
2. Central Processing Unit (CPU)
3. Output device

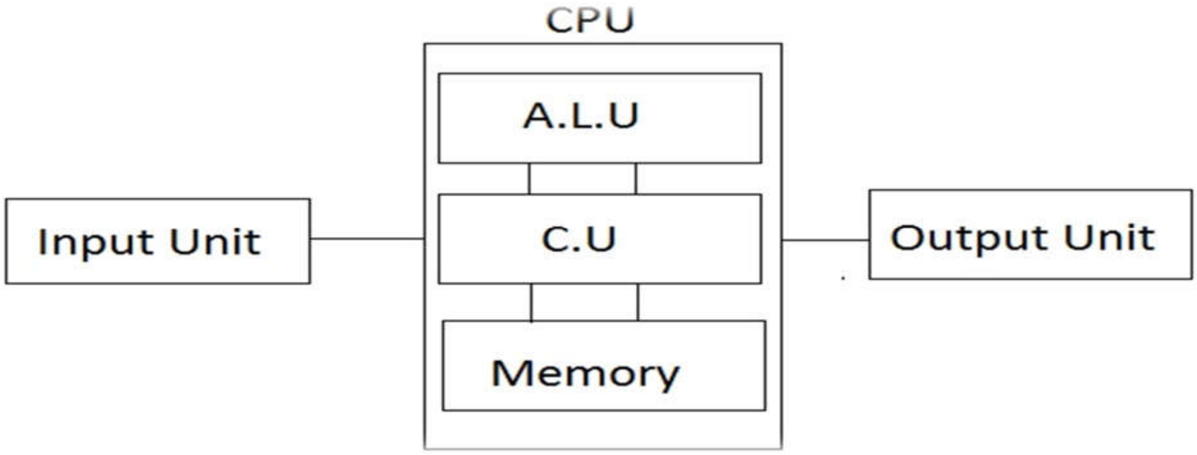


Fig: Block diagram of computer

The functions of these units can be summarized as:

1. **Input device:** Any device which reads information from input media and enters to the computer in a coded form.
   E.g. keyboard, Mouse etc.

2. **CPU**
   a. *Memory unit* : Stores program and data
   b. *Arithmetic Logic unit* : Performs arithmetic and logical functions
   c. *Control Unit* : Interprets program instructions and controls the input and output devices

3. **Output device**: The result obtained after processing is considered output. The output device decodes information and presents it to the user.
   E.g. Monitor, Projector etc.

2.5. Advantages of computer/(s)

1. **High speed:** Computers have the ability to perform routine tasks at a greater speed than human beings. They can perform millions of calculations in seconds.

2. **Accuracy:** Computers are used to perform tasks in a way that ensures accuracy.

3. **Storage:** Computers can store large amount of information. Any data or instructions stored in the memory can be retrieved by the computer at very high speed.

4. **Automation:** Computers can be instructed to perform complex tasks automatically which increases the productivity.

5. **Diligence:** Computers can perform the same task repeatedly & with the same accuracy without getting tired.

6. **Versatility:** Computers are flexible to perform both simple and complex tasks.

7. **Cost effectiveness:** Computers reduce the amount of paper work and human effort thereby reducing costs.

2.6. Limitations of computers

1. Computers need clear & complete instructions to perform a task accurately. If the instructions are unclear the results will be inaccurate.
2. Computers cannot think.
3. Computers cannot learn by experience.

2.7. Types of computers

A **personal computer** is a computer that can perform all of its input, processing, output and storage activities by itself. A personal computer contains a processor, memory and one or more input, output and storage devices. Personal computers are also called *microcomputers.*

Two types of personal computers are desktop computers and notebook computers.

- A *desktop computer* is designed so that the system unit, input devices, output devices and any other devices fit entirely on a desk or table.

- A *notebook computer* also called a *laptop computer* is a portable personal computer small enough to fit on your lap. Notebook computers are thin and lightweight yet they are as powerful as the average desktop computer.

Note: A *netbook* which is a type of notebook computer is smaller, lighter & often not as powerful as a traditional notebook computer. Most netbooks cost less than traditional notebook computers.

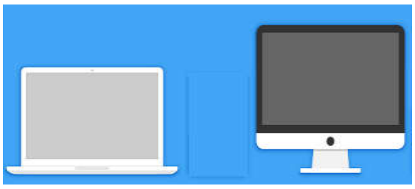


Fig: Notebook & Desktop

2.7.1. Workstations

A workstation is a specialized single user computer that typically has more power & features than a standard desktop or PC.

These machines are popular among scientists, engineers and animators who need a system with greater than average speed & the power to perform sophisticated tasks.

Fig: Workstations

2.7.2. Mainframe computers

Mainframe computers are large computer system that has the capability to support more powerful peripheral devices and terminal.

It is multiuser, multiprogramming and high performance computers & operate at a very high-speed.

These types of computers are used for complex scientific calculations, large data processing application and for complex graphics applications.

Fig: Mainframe Computers

2.7.3. Mini computers

Minicomputers got their name because of their small size compared to other computers. The capabilities of mini computers are somewhere between the mainframes & personal computers. Therefore, they are also called as *midrange computers*. It is a multiuser computer capable of supporting hundreds of users simultaneously. The minicomputers can handle very large input and output when compared to microcomputers.

2.7.4. Super computers

Supercomputers are very expensive and are employed for specialized applications that require immense amount of mathematical calculations. For example, weather forecasting requires a supercomputer. Other uses of supercomputers include animated graphics, complex calculations, nuclear-energy research and petroleum exploration.

The main difference between a supercomputer and a mainframe is that a supercomputer channels all its power into executing few programs as fast as possible whereas a mainframe uses its power to execute many programs concurrently.

Fig: Supercomputers

2.7.5. Tablet PC

Tablet PC offers all the functionalities of notebook PC but they are lighter and can accept input from a special pen called stylus or digital pen that is used to tap or write directly on the screen.

Fig: Tablet PC

2.7.6. Handheld computers

A **handheld computer**, sometimes referred to as an *Ultra-Mobile PC* (*UMPC*), is a computer small enough to fit in one hand. It provides functionality approaching that of a laptop computer. Features of modern handhelds include calendar and diary organizing, word processing, data management, remote access to office network, internet access, wireless access, messaging, etc. Hand held computers are also called as Personal Digital Assistant (PDA).

Fig: Handheld computers

2.7.7. Smart phones

Smartphones are electronic handheld device that has the functionality of a mobile phone and PDA. This is achieved by integrating mobile phone capabilities with the more common features of a PDA. Smartphones allow users to store information, e-mail and install programs along with mobile phone in one device.

Fig: smartphones

2.8. Components of a Computer

2.8.1. Memory

Memory consists of electronic components that store instructions waiting to be executed by the processor, data needed by those instructions and the processed results Memory usually consists of one or more chips on the motherboard or some other circuit board in the computer. Memory stores three basic categories of items

1. the operating system and other system software that controls or maintains the computer and its devices
2. application programs that carry out a specific task such as word processing and
3. The data being processed by the application programs and resulting information.

Types of Memory:

The memory can be classified into two major types of memory:

- **Volatile**
  - When the computer power is turned off volatile memory loses its contents.
  - RAM is the most common type of volatile memory.

- **Non-volatile**
  - Non-volatile memory by contrast does not lose its contents when power is removed from the computer.
  - Examples of non-volatile memory include ROM, flash memory, HDD etc.

Thus, volatile memory is temporary and non-volatile memory is permanent.

Note: Volatile memory is also collected as part of investigation for conducting volatile memory analysis. This gives active artefacts of the system which will be very much useful for investigation.

2.8.2. Input devices

Key board: A computer keyboard contains keys you press to enter data into the computer. It is also known as primary input device. Today, the most widely used keyboard consists of a 104-key layout with additional keys used to access the Internet, music, and other frequently used programs known as multimedia keyboard. There are different types of keys on the keyboard. The keys are categorized as:

1. Alphanumeric keys including letters & numbers.
2. Punctuation keys such as colon (:) semicolon (;) Question mark (?) Single & double quotes etc.
3. Special keys such as arrow keys, control keys, function keys (F1 to F12), Home, End etc.

Fig: Keyboard

Mouse

It is a device that controls the movement of the cursor on a monitor. A mouse will have two buttons on its top. The left button is the most frequently used button. Some mice will be having a wheel between the left and right buttons. This wheel enables us to smoothly scroll through the screen. As we move the mouse, pointer on the monitor moves in the same direction. Mouse cannot be used for entering the data. It is only useful to select the options on the screen.

Types of mouse:

There are three basic types of mouse:

1. Mechanical
2. Optomechanical
3. Optical

Mechanical mouse:

A mechanical mouse has a rubber or metal ball on its underside that can roll in all directions. Mechanical sensors within the mouse detect the direction of the rolling ball and moves the screen pointer accordingly.

Optomechanical mouse:

This mouse is similar to the mechanical mouse except that it uses optical sensors to detect the movement of the ball on the mouse pad.

Optical mouse:

Optical mouse uses Light-Emitting Diodes (LED) or laser as a method for tracking the cursor movement on screen which makes them more proficient than its predecessors.

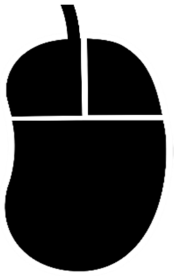


Fig: Mouse

Trackball

A trackball is a stationary pointing device with a ball on its top or side. To move the pointer using a trackball you rotate the ball with your thumb, fingers, or the palm of your hand.

Fig: Track Ball

Pointing stick

A *pointing* device that looks like a pencil eraser located in the center of a computer keyboard. Some notebook computers include a pointing stick to allow a user to control the cursor movement on screen.

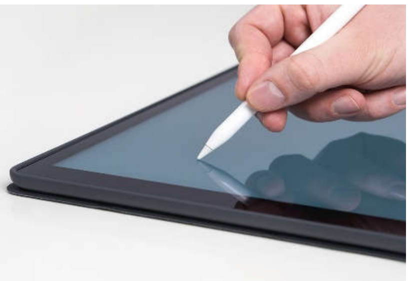


Fig: Pointing stick

Touchpad:

A touchpad is a small, flat, rectangular pointing device controlling the pointer on a display screen by sliding the finger along a touch-sensitive surface. Some touchpads have one or more buttons around the edge of the pad that work like mouse buttons. Most touchpads when tapped on the pad will imitate mouse operations such as clicking.

Fig: touchpad

Scanners

Scanner is an input device that accept paper document as input. Scanner is used to input/feed the data directly into the computer from the source document (e.g. Hard copy of documents, Images etc.,) without copying or typing the data. The input data to be scanned can be a picture or text on a paper. It is an optional input device and uses light as an input source to convert image into electronic form that can be stored on a computer.

Types of scanners

Flatbed Scanners: The flatbed scanner is the most popular scanner today. In this type of scanner the paper is put on a flat glass plate and the scanner head moves across the page inside the body of the scanner.
It is also the most common type of scanner. Flatbed scanners gained there popularity since they are inexpensive and produce the best results for scanning single photographs or documents.

Fig: Scanners

Sheet-fed Scanners: A sheet-fed scanner is similar to a flatbed scanner but instead of a moving scan head the paper is moved automatically through the scanner across a stationary scan head. There are sheet-feeder attachments for some flatbed scanners that will turn them into sheet-fed scanners.
The main advantage of a sheet-fed scanner over a flatbed scanner is speed. Sheet-fed scanners are designed to scan large numbers of documents in a short span of time.

Photo Scanners: As their name implies photo scanners are special purpose device useful for creating electronic images of photographs. They are smaller in size since it is designed to work primarily with the size of photograph.

Handheld Scanners: The Handheld scanners are compact portable scanner designed to capture text and other data while on the go. To use a handheld scanner you move the scanner over the object that you want to scan. Hand held scanners don't offer the picture quality and convenience of a flatbed scanner.

Fig: Handheld Scanners

Warning: To access the prints a little faster, manufacturers adds memory to all the latest printers which accepts the document and prints it later even when it is offline. This buffer can store lot of important and confidential documents which you have scanned or printed.

Microphone: An acoustic sensor that provides input by converting sound into electrical signals i.e. voice input is the process of entering input by speaking into a microphone. The microphone may be a stand-alone peripheral that sits on top of a desk or built in the computer or device or in a headset.

Fig: Microphone

Light pen: A light pen is a hand held electro optical pointing device which when touched or aimed closely at connected computer monitor will allow the computer to determine where on that screen the pen is aimed. Light pens give user the full range of mouse capabilities without the use of a pad or any horizontal surface.

Bar code readers:
Bar code reader also known as barcode scanner is an optical reader that uses laser beams to read bar codes by using light patterns that pass through the bar code.

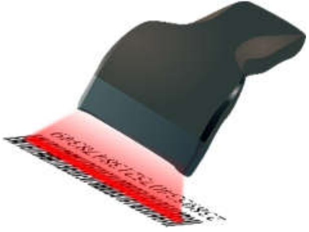


Fig: Bar code reader

2.8.3. Output devices

Display devices:

CRT (Cathode Ray Tube) monitors: CRT monitors were popular for computing for many years and were also popular as television screens. Typically, they have curved screens but there are flat screen versions as well. CRT monitors displays the image by using an electron gun that shoots electrons at the phosphors covering the back of the screen causing those areas of the screen to glow.

LCD: Liquid Crystal Display (LCD), a popular flat-display type found on laptops for many years is now a popular choice for display with desktop computers and TVs.
An LCD has two sheets of material surrounding a liquid that contains crystals that act as pixels for the display. Each crystal has a red, green and blue cell illuminated by an electrical charge hitting the crystal which then creates the onscreen image.

LCD monitors and LCD screens typically produce color using either active-matrix or passive-matrix technology.
An active-matrix displays also known as a TFT (thin-film transistor) display which uses a separate transistor to apply charges to each liquid crystal cell and thus displays high-quality color.

A passive-matrix display uses fewer transistors, requires less power and is less expensive than an active-matrix display.

OLED: *Organic LED* (*OLED*) uses organic molecules that produce an even brighter easier-to-read display than standard TFT displays. OLEDs are less expensive to produce, consume less power and can be fabricated on thin flexible surfaces.

PLASMA: Plasma displays are flat displays like LCDs but use a different approach for creating the image onscreen. Plasma displays create the image by having small cells of gas sitting between two plates of glass. An electrical charge is applied to the cells of gas which then causes the cells to light.

Fig: Monitors

Projector: A data projector is a device that takes the text and images displaying on a computer screen and projects them on a larger screen so that an audience can see the image clearly.

Fig: Projector

Printer: A printer is used to transfer data from a computer onto paper. The paper copy obtained from a printer is often referred as printout.

Types of printers:

Laser Printer: A laser printer is a high-speed, high-quality nonimpact printer i.e. keys don't strike the paper. It is the most popular type of printer because it is fast, reliable and offers the best-quality printout of the three types of printers. A laser printer gets its name because it uses a laser beam in the printing process.

Fig: Laser Printer

Ink Jet Printers
Inkjet printers offer the next highest level of print quality and are relatively cheap compared to laser printers. Inkjet printers are great for home use or small office environments that don't have large print jobs.

Inkjet printers don't use toner like a laser printer instead they use ink cartridges. The ink cartridge contains all the working elements needed to get an image from the computer onto a sheet of paper.

Dot Matrix Printer
Dot matrix printers are considered as *impact* printers since they physically strike an inked ribbon with a metal pin to put characters on paper. The ink is transferred to the paper as closely shaped dots that form each character. More the pins better the print quality.

Comparison of different types of printers:

Sl. No.	Type	Style of printing	speed
1	Dot Matrix	Prints the character in dotted pattern through printer ribbon using either 24 pin or 9 pin	200/300 to 700 Character per sec
2	Ink Jet printer	Work by spraying ionized ink	90 Character per sec
3	Laser printer	Also called page printer. Uses laser beam to produce an image.	6 to 12 Pages Per Minute

Speakers and headphones: An audio output device is a component of a computer that produces music, speech or other Sounds such as beeps. Two commonly used audio output devices are speakers and headphones.

Fig: speakers & headphones

2.8.4. Storage devices

Storage devices hold data, instructions and information for future use. A computer keeps data, instructions, and information on storage media. Examples of storage media are USB flash drives, hard disks, optical discs, RAM etc.

2.8.4.1. Primary storage:

Primary storage is a storage location that holds memory for short periods of times while the computer running. For example, computer RAM and cache are both examples of a primary storage device. This storage is the fastest memory in your computer and is used to store data while it's being used. Primary storage is alternatively referred as internal memory, main memory and primary memory.

RAM (Random Access Memory): RAM, also known as main memory, consists of memory chips (Integrated Chips) that can be read from and written to the processor and other devices. When you turn on power to a computer certain operating system files (such as the files that determine how the desktop appears) load into RAM from a storage device such as a hard disk. These files remain in RAM as long as the computer has continuous power. The additionally requested programs and data are also loaded into RAM from storage.

Fig: RAM

The main types of RAM include static RAM (SRAM) and dynamic RAM (DRAM). Static RAM is more expensive and has more capacity for storage than dynamic RAM that has to be refreshed more often and is thus slower.

ROM (Read Only Memory): Read-only memory refers to memory chips storing permanent data and instructions. The data on most ROM chips cannot be modified hence the name read-only. ROM is non-volatile, which means its contents are not lost when power is removed from the computer.
Manufacturers of ROM chips often record data, instructions or information on the chips when they manufacture the chips. These ROM chips called *firmware* contain permanently written data, instructions or information.

PROM (programmable read-only memory): PROM Chip is a blank ROM chip on which a programmer can write permanently. Programmers use microcode instructions to program a PROM chip. Once a programmer writes the microcode on the PROM chip it functions like a regular ROM chip and cannot be erased or changed.

Erasable programmable ROM (EPROM):

EPROM is a special type of memory that retains its contents until it is exposed to ultraviolet light. The ultraviolet light clears its contents making it possible to reprogram the memory.

EEPROM (electrically erasable programmable read-only memory)

EEPROM is a special type of PROM that can be erased by exposing it to an electrical charge. Like other types of PROM EEPROM retains its contents even when the power is turned off.

Flash ROM:

Flash ROM is a type of non-volatile memory that can be erased electronically and rewritten similar to EEPROM. Most computers use flash memory to hold their start-up instructions because it allows the computer easily to update its contents.

Cache

Most of the today's computers improve their processing times with cache (pronounced cash) is an extremely fast memory that is built into a computer's central processing unit (CPU) or located next to it on a separate integrated chip. Cache helps in speeding up the processes of the computer because it stores frequently used instructions and data. When the processor needs an instruction or data it searches first in cache and then in RAM.

2.8.4.2. Secondary storage:

It is a storage medium that holds information until it is deleted or overwritten regardless if the computer has power. It is also referred to as *external memory or auxiliary storage.*

Hard drive

This is the main storage media for most computer systems. It holds the boot files, operating system files, programs and data.

SCSI (Small Computer Systems Interface)

SCSI is an electronic interface that originated with Apple computer systems and migrated to other systems. It is a high-speed, high-performance interface used on devices requiring high input/output such as scanners and hard drives. The SCSI BIOS is intelligent BIOS that queues read/write requests in a manner that improves performance making it the choice for high-end systems.

IDE (Integrated Drive Electronics) controller

IDE is a generic term for any drive with its own integrated drive controller. The most commonly used IDE controller is known as ATA (Advanced Technology Attachment). The IDE interface today is called ATA and the two names will often be used interchangeably. Two IDE connectors are found on the motherboard one labelled primary IDE and the other secondary IDE.

Each is capable of handling two IDE devices (hard drive, CD, DVD) for a maximum of four IDE devices. Of the two devices on the same IDE ribbon cable (40-pin header connector) one is the *master* and the other is the *slave.* One places jumpers on pins to designate the master or slave status.

Typically the boot hard drive will be attached to the primary controller and it is the master if two devices are present on that IDE channel.

Fig: IDE HDD

SATA (Serial Advanced Technology Attachment)

SATA uses serial circuitry which allows data to be sent initially at 150 MBps. Enhancements in the SATA have increased the data transfer speed up to 600 MB/s. A SATA bus uses a small 7-pin connector and a thin cable for connectivity.

RAID (Redundant Array of Inexpensive Disks)

RAID means Redundant Array of Independent Drives (or Disks), and it is also known as Redundant Array of Inexpensive Drives (or Disks). Thus, the letter I can mean inexpensive or independent and the letter D can mean drives or disks.

A RAID is an array of two or more disks combined in such a way as to increase fault tolerance.

Fig: RAID

Optical Disks:

An optical disc is a flat, round, portable metal disc with a plastic coating. CDs, DVDs and Blu-ray Discs are three types of optical discs:

CD Compact Disc

CD is a multisession optical disc on which users can write their own items such as text, graphics, and audio. *Multisession* means you can write on part of the disc at one time and another part at a later time.

CD drives use laser beams to read indentations and flat areas as 1s and 0s.The data is formatted into a continuous spiral emanating from the center to the outside. A CD allows you to store 700 to 800 MB of data.

DVD-ROM (Digital Versatile Disc)

DVD stores data, instructions, and information in a slightly different manner and thus achieves a higher storage capacity than CD. DVD quality also far surpasses that of CDs because images are stored at higher resolution. Widely used DVDs are capable of storing 4.7 GB to 17 GB depending on the storage techniques used.

Blu-ray Disk: Blu-ray Disc (BD) is the name of a new optical disc format jointly developed by the Blu-ray Disc Association (BDA). The format was developed to enable recording, rewriting and playback of high-definition video (HD) as well as storing large amounts of data. The format offers more than five times the storage capacity of traditional DVDs and can hold up to 25GB on a single-layer disc and 50GB on a dual-layer disc.

Flash Memory: Flash memory is a type of non-volatile memory that can be erased electronically and rewritten.

Flash memory chips also store data and programs on many mobile computers and devices, such as smart phones, portable media players, PDAs, printers, digital cameras etc.

A **memory card** is a removable flash memory device, usually no bigger than 1.5" in height or width that you insert and remove from a slot in a personal computer, game console, mobile device or card reader/writer.

A **USB flash drive** is a flash memory storage device that plugs in a USB port on a computer or mobile device.

2.8.5. The Microprocessors (CPU) and Motherboard

The processor also called a CPU (central processing unit) is the electronic component that interprets and carries out the basic instructions that operate the computer. The processor significantly impacts overall computing power and manages most of a computer's operations.

Most processor chip manufacturers now offer multi-core processors. A processor core or simply core contains the circuitry necessary to execute instructions. The operating system views each processor core as a separate processor. A *multi-core processor* is a single chip with two or more separate processor cores. Two common multi-core processors are *dual-core* and *quad-core*. A dual-core processor is a chip that contains two separate processor cores. Similarly, a quad-core processor is a chip with four separate processor cores.

The **motherboard** sometimes called a system board is the main circuit board of the system unit. Many electronic components are attached to the motherboard. Many current motherboards also integrate sound, video and networking capabilities.

Motherboard is the largest printed circuit card within the computer case typically contains

- CPU socket
- BIOS
- CMOS
- RAM memory slots
- Integrated Drive Electronics (IDE) controllers
- Serial Advanced Technology Attachment (SATA) controllers
- Universal Serial Bus (USB) controllers
- Accelerated Graphics Port (AGP)
- Peripheral Component Interconnect (PCI)Express video slots PCI or PCI Express expansion slots

BIOS Chip

Apart from processor, the most important chip on the motherboard is the Basic Input/ Output System (BIOS) chip. This special memory chip contains the BIOS software that tells the processor how to interact with the rest of the hardware in the computer.

CMOS

The CMOS is the Complementary Metal Oxide Semiconductor. This is where the basic information about the computer's configuration is stored. These settings are preconfigured in BIOS which include:

- Which hard drives and floppy drives are present
- How much memory is installed
- Whether a keyboard is required to boot
- The type of mouse installed (PS/2 or USB)
- What is the power-on password and whether it is required to boot up the system
- The date and time

2.8.6. Expansion Slots

Expansion slots are used to install various devices in the computer to expand its capabilities. Some expansion devices that might be installed in these slots include video, network, sound etc.

PCI Slots

PCI provides the interconnection between the CPU and attached devices. The plug-and-play functionality of PCI enables the host to easily recognize and configure new cards and devices. PCI slots are easily identified on the motherboard as the small white slots usually located alongside the AGP slot.

AGP Slots

Accelerated Graphics Port (AGP) slots are very popular for video card use. AGP slots were designed to be a direct connection between the video circuitry and the PC's memory. They are usually brown & are located right next to the PCI slots on the motherboard.

PCI Express: *PCIe* expansion slot architecture that is being used by most of the motherboard manufactures. It was designed to be a replacement for AGP and PCI. It has the capability of being faster than AGP while maintaining the flexibility of PCI.

Switch Mode Power Supply (SMPS)

Many personal computers plug in standard wall outlets which supply an Alternating Current (AC) of 220 to 240 volts. This type of power is unsuitable for use with a computer which requires a Direct Current (DC) ranging from 5 to more than 15 volts. The power supply is the component of the system unit that converts AC power into DC power. Different motherboards and computers require different wattages on the power supply. Notebook computers including netbooks and Tablet PCs can run using either batteries or a power supply.

Heat sink and fan: Heat sink and fan are attached to the CPU to keep it cool. The heat sink interfaces directly with the processor. The heat sink consists of a high-thermal conductance material whose job is to draw the heat from the processor and to dissipate that heat into the surrounding with the assistance of the fans.

2.9. Unit of Measurement:

All information represented inside a computer system are in binary. Thus, the basic unit of memory is a bit (binary digit: 0 or 1). To store a character computer requires 8 bits or 1 byte. This is called the word length. Hence, the storage capacity of the computer is measured in the number of words it can store and is expressed in terms of bytes.

Manufacturers state the size of memory and storage devices in terms of the number of bytes available for storage by the chip or device.

Sl.no	Unit	Abbreviation	value
1	Bit	b	0 or 1
2	Byte	B	8 bits
3	Kilobytes	KB	1024 bytes
4	Megabytes	MB	1024KB
5	Gigabytes	GB	1024MB
6	Terabytes	TB	1024GB

2.10. Types of Software:

The whole gamut of software present in a computer system can broadly be classified into two categories

2.10.1. System software:

System software consists of the programs that control or maintain the operations of the computer and its devices. System software serves as the interface between the user, the application software and the computer's hardware. Two types of system software are operating systems and utility programs. E.g. operating system, device drivers

An *Operating System* (OS) is a set of programs containing instructions that work together to coordinate all the activities among computer hardware resources. E.g. windows XP, 7, 8, Linux, Macintosh etc.

A *utility program* also called a *utility* is a type of system software that allows a user to perform maintenance-type tasks usually related to managing a computer, its devices, or its programs. E.g. antivirus, firewalls, uninstallers etc.

2.10.2. Application software:

Program designed to make users more productive or assist them with personal tasks. Application software has a variety of uses:

1. To make business activities more efficient
2. To assist with graphics and multimedia projects
3. To support home, personal and educational tasks
4. To facilitate communications

A widely used type of application software's are Web browsers which allows users to access and view Web pages or access programs. Other popular application software includes word processing software, spreadsheet software, database software and presentation software
E.g. MS-office, internet explorer, Nero etc.

2.11. Ports and Connectors

A *port* is the point at which a peripheral attaches to or communicates with a system unit so that the peripheral can send data to or receive information from the computer. An external device, such as a keyboard, monitor, printer, mouse, and microphone, is often attached by a cable to a port on the system unit (CPU).The front and back of a system unit on a desktop personal computer contain many ports.

A *connecto*r joins a cable to a port. A connector at one end of a cable attaches to a port on the system unit and on the other end to a port on the peripheral.
Most connectors and ports are available in one of two genders: male or female.
Male connectors and ports have one or more exposed pins. Female connectors and ports have matching holes to accept the pins on a male connector or port.

USB port: Universal serial bus port can connect up to 127 different peripherals. Devices that connect to a USB port includes mouse, printer, digital camera, scanner, speakers, portable media player, optical disc drive, smart phone, PDA, game console and removable hard disk. Personal computers typically have six to eight USB ports on the front and/or back of the system unit.

eSATA Port: An **eSATA port** or *external SATA port* allows you to connect an external SATA (Serial Advanced Technology Attachment) hard disk to a computer. SATA hard disks are popular because of their fast data transmission speeds. eSATA connections provide up to six times faster data transmission speeds than external hard disks attached to a computer's USB.

Serial Ports: a serial port is a type of interface that connects a device to the system unit by transmitting data one bit at a time. Some modems that connect the system unit to a telephone line use a serial port because the telephone line expects the data in a specific frequency.

Audio ports are used to connect speakers or microphones to the computers.

Network ports are used to connect computer to a network via a network cable typically a cable using RJ45 connector.

HDMI (*High-Definition Multimedia Interface***) Ports:** *HDMI* is an all-digital *connector* that can carry high-*definition* video and several digital audio channels all on the one cable.

2.12. Boot process

Booting is a process or set of operations that loads and hence starts the operating system, starting from the point when user switches on the power button.

1. Power supply sends signal to components in system unit.

2. The CPU of the PC executes instructions located at BIOS stored in ROM to start the computer.

3. BIOS performs a Power on Self-Test (POST) to check components such as mouse, keyboard and expansion cards.
4. The BIOS goes through pre-configured list of boot device sequence.

5. Result of the POST are compared to data in the CMOS chip. The CMOS chip stores configuration information about the computer, such as the amount of memory, type of disk drives, keyboard, monitor, current date and time and other start-up information. It also detects any new devices connected to the computer. If something is missing, computer will alert user with a tone or an onscreen message.

6. If the POST completes successfully, the BIOS searches for specific operating system files called system files. The BIOS may look first to see if a USB flash drive plugged in a USB port or a disc in an optical disc drive contains the system files or it may look directly on drive C (the designation usually given to the first hard disk) for the system files.

7. Once located the system files load into memory (RAM) from storage (usually the hard disk) and execute. The operating system in memory takes control of the computer.

8. Operating system loads configuration information and displays desktop on screen. OS executes any program in the start-up folder and the computer is ready to use.

How Data is stored in a computer?

The main data storage in computers is hard disks. It is a sealed aluminium box with controller electronics attached to one side. The electronics control the read/write mechanism and the motor that spins the platters.

The hard disk holds operating system, boot files, Programs and user data. The data in the hard disk are stored in consecutive 0's and 1's.

Hard disk consists of series of platters which revolves at speed ranging from 4,800 to 15,000 revolutions per minute (RPM). The platters are magnetized and are accessed by the heads moving across their surfaces as they spin.

The heads can read & write detecting the changes in polarity with positive charge being 1 and negative 0. A disk drive uses a rapidly moving arm to read and write data across a flat platter coated with magnetic particles. Data is transferred from the magnetic platter through the R/W head to the computer.

Platters are further separated in to the *tracks* and s*ectors* where tracks are concentric circles. Each track is divided into smaller units called *sectors* which are pie-shaped segments on a track.

A sector is the smallest individually addressable unit of storage. Sectors are grouped either at the drive or the operating system level called clusters.
Data can be stored after formatting the hard disk. Formatting is the process of establishing the location of sectors, tracks and file systems.

Note: Hard disk schematics **or** disk geometry are very important for a forensic examiner to understand how the hidden data is stored and can be retrieved.

2.13. Internet Concept

The origins of the Internet date back nearly 40 years, with the U.S. military's funding of a research network dubbed Arpanet in 1969. Since then, the Internet has undergone more than just a name change. The number of computers connected to the Internet has grown exponentially, while the number of users has risen from a handful of computer scientists to more than 4 billion consumers.

The Internet is the largest *computer network* in the world, connecting more than a billion computer users. It is a global collection of computer networks that are connected together by the devices such as routers, switches etc. It uses a common set of protocols for data transmission known as TCP/IP (Transmission Control Protocol / Internet Protocol). They do this through unique identification numbers called Internet Protocol Addresses (IP addresses). There are many different tools used on the Internet to make this possible. Probably the most popular of all Internet tools is the World Wide Web. The primary purpose of the Internet is to facilitate the sharing of information.

Generally to exchange the information it requires the client and servers. Internet resources information and services that are provided through host computers, known as servers. A server is a physical computer dedicated to run services to serve the needs of other computers. Depending on the service that is running, it could be an application file server, database server, web server, print server, or media server.

A **computer network** often simply referred to as a network, is a collection of computers and devices interconnected by communication channels that facilitate communication and allows sharing of resources and information among interconnected devices. Put more simply, a computer network is a collection of two or more computers linked together for the purposes of sharing information, resources, among other things.

Why Networking?

- Consolidate network storage
- Share Peripherals
- Centralization- Computers can be managed centrally

- Increase communication internally & externally
- Time - it is much faster to install an application once on a network - and copy it across the network to every workstation

Use of Internet

Today internet technology has become ubiquitous. The network which we are using at home are the same networking technologies, protocols and services that are used by businesses, Government etc. The e-commerce industry is entirely dependent on internet and people are doing transaction worth billions of dollars worldwide using internet. The world is going digital adopting information technology in day to day life. Spurt in the use of smartphone with internet connectivity have increased activities such as buying groceries, paying bills, online banking, e-wallets (e.g. PayTM, MobiKwik etc.,)

Wired and wireless Internet; concept of Wi-Fi

Networks can be wired or wireless with most networks being a mixture of both. A Wired network differs from wireless which use radio waves rather than transmitting signals over the cables. A wireless LAN (WLAN or Wi-Fi) is a data transmission system designed to provide location-independent network access between computing devices by using radio waves.

Wi-Fi stands for Wireless Fidelity. It is a technology for wireless local area networking with devices based on IEEE 802.11 standards. Wi-Fi compatible devices can connect to the internet via WLAN network and a wireless access point. There is a plethora of standards under the IEEE 802 (LAN/MAN), 802.11a, b, g, n etc.

IEEE Standard	Frequency/Medium	Speed
802.11	2.4GHz RF	1 to 2Mbps
802.11a	5GHz	Up to 54Mbps
802.11b	2.4GHz	Up to 11Mbps
802.11g	2.4GHz	Up to 54Mbps
802.11n	2.4GHz/5GHz	Up to 600Mbps

Fig: Wireless standards

2.14. Common Networking devices

Hub

A hub is a small, simple, inexpensive device that joins multiple computers together. Many network hubs available today support the Ethernet standard.

Fig: Hub

Hub broadcasts all the data packets received from one port to all available ports. That means a packet sent via one computer to a certain destination computer goes to each and every computers which are connected to the same Network.

Repeaters

A repeater is a network device that is used to regenerate or replicate signals that are weakened or distorted by transmission over long distances. The purpose of a repeater is to extend the LAN segment beyond its physical limits. These days, wireless repeaters are gaining popularity to extend or strengthen the radio signals.

Fig: Repeater

Modem

A modem (modulator-demodulator) converts digital signals (computer signals) from the computer into analogue signals for transmission and vice versa for reception over a telephone line.

[redacted]

Fig: Modem

Switch

A Switch is a Networking Device which has some intelligence as compared to Network Hub.
It binds IP with MAC in communication.
It doesn’t broadcast the data packet to all the computer in the network but to the destination computer

Fig: Switch

Wireless Access Point (WAP)

A wireless access point is a device that allows wireless devices to connect to a network. They are specially configured nodes on wireless local area networks (WLANs) to act as a central transmitter and receiver of WLAN radio signals.

The WAP can also bridges WLANs with a wired Ethernet LAN and also scales the network to support more clients.

Router

Router is a Network device which sends the data packets from one network to another.
In simple terms Routers is a bridge between two Networks.
It directs traffic over internet.
Typically, two types of packets arrive at a router: packets to be forwarded to another network or packets destined to the router itself.
Router reads the destination IP address of the data packet & accordingly transmits the data to the destination computer.

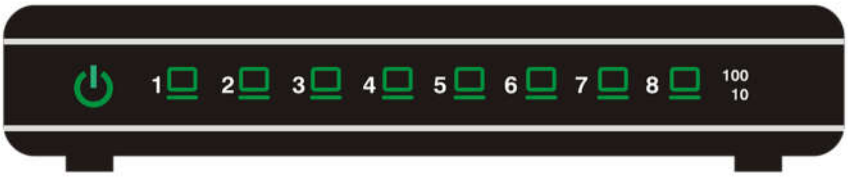


Fig Router

Firewalls

It is one of the most important components of a modern computer network. Its job is to control traffic both in & out of the network. Generally firewalls are deployed at network perimeters. This provided some measure of protection for internal hosts.

Network designers now often include firewall functionality at places other than the network perimeter to provide an additional layer of security, as well as to protect mobile devices that are placed directly onto external networks.

There are two basic types of firewalls

- Hardware firewalls
- Software firewalls

Hardware firewalls are exactly what the name implies i.e. a hardware device is placed somewhere in the network. Once placed it receives and analyzes packets traveling in and out of the network.
Software based firewalls are installed on an existing device such as a workstation or server. These applications perform the same tasks as hardware based solutions, namely analyzing

network packets to determine whether or not they should be allowed to continue to their intended destination

2.15. Email Concepts

Email is also called as electronic mail. It is similar to postal service mail, but much quicker to use. For instance, with postal service mail, you write out a letter and put it inside an envelope, put a stamp on the envelope, take the envelope to a mailbox and wait several days for the envelope to be delivered and read. Email is quicker. Open your email program on a computer with a couple of mouse clicks. Compose a letter in the text message box. Type in the email address of your receiver. Click on Send. The person receives the email almost instantly.

Today's email systems are based on a store-and-forward model. Email servers accept, forward, deliver, and store messages. Neither the users nor their computers are required to be online simultaneously; they need to connect only briefly, typically to a mail server or webmail interface, for as long as it takes to send or receive messages. Functions such as email exchange are built on the client-server model.

Mail Server

A mail server is an application that receives an incoming e-mail from local users and remote senders and forwards outgoing e-mail for delivery. A computer dedicated to running such applications is also called a mail server. Microsoft Exchange, Gmail, Exim and send mail are among the more common mail server programs. The mail server works in conjunction with other programs to make up what is sometimes referred to as a messaging system. A messaging system includes all the applications necessary to keep e-mail moving as it should. When you send an e-mail message, your e-mail program, such as Outlook or webmail, forwards the message to your mail server, which in turn forwards it either to another mail server or to a holding area on the same server called a message store to be forwarded later. As a rule, the system uses SMTP (Simple Mail Transfer Protocol) or ESMTP (extended SMTP) for sending e-mail, and either POP3 (Post Office Protocol 3) or IMAP (Internet Message Access Protocol) for receiving e-mail.

2.15.1. How Does Email server work?

E-mails are communicated between two or more users. An e-mail can be composed by a sender using outlook, webmail or Application using computers, smartphones, tablets etc., Once the sender clicks the send button e-mail will be sent to the mail server. Every e-mail service providers (ESP) have their own dedicated e-mail servers which transfer e-mail from one part of the world to another.

When the mail server receives the e-mail message from the sender the destination address is verified, if the ESP is of the same company then the mail server can directly send it to the recipient’s mailbox. If the recipients ESP is different, the sender's e-mail server will look for the recipient's e-mail server and send to that e-mail server. The receivers e-mail server then pushes the e-mail to the recipient. As the message travels through the network, an abbreviated record of the e-mail journey is recorded in an area of message called the header.

CHAPTER-III

Drafting a report & Information Gathering

CHAPTER-III: Drafting a report & Information Gathering

Why Should I read this Chapter?

After reading this chapter, you would be able to:

- Understand the basic computer fundamental and its components.
- Understand the various sources of information in cybercrime Investigations

3.1. Drafting a clear report

It is very important for every Investigating Officer (IO) to do a pre-investigation assessment for each cybercrime/incident that is reported. In most general cases, before the complainant approaches the police officer or any agency for reporting their problems, they may have made some attempts to set the things right all by themselves or with the help of their family, friends or some other persons. However, these very acts may result in the destruction of crucial digital evidence(s). Similarly, the criminal act may be a crime in progress, which can sometimes potentially cause further damage. It is also possible that the complainants in their anxiety or due to ignorance may not disclose the full facts at the outset. All these elements will have an impact on the outcomes of investigations.

Depending on the nature of each case reported, the IO should collect necessary information from the complainant(s) / victims as part of the pre-investigation, to appreciate the full scope of the case and, the possible outcomes. This will help the IO to build the plan of action/next steps in the investigation. Investigators and technical personnel are aware of the fact that, the digital evidence is very critical and volatile. For successful investigations, it is very much required to protect and collect the right evidence and plan what action needs to be taken further.

The pre-investigation should consider various aspects of crime including the location and the circumstances. A set of questions needs to be asked by the IOs to draw information which depends on the nature of the case, will enable them to quickly estimate the scope of case and damage happened to the complainant. Such a questionnaire will help the investigating officer to decide on the priority actions that are necessary for the interest of the securing all the digital evidence without destruction, loss or tampering.

Questions are drafted based on the type of case:

- In the First place, is it a crime as per IT Act, 2000
- It is advisable to consult a fellow cybercrime cell team, Legal cell or any other expert in this domain before issuing a first information report. This will help an IO to determine which section he should use under the law to register a case.
- Be sure regarding the fraudulent or dishonest intentions of the alleged suspect as all those needs to captured and drafted under the report.
- Include the nature of crime and modus operandi of the cybercrime in detail.
- Indicate all the details IO can identify from the complaint like,
    - IP address in case of e-mail and Internet.
    - Profile name or username in case of social networking abuse.
    - Bank details/Internet banking, branch, etc., in case of online fraud.
    - Credit card details and nature of the purchase, etc., in case of card fraud, etc.

Some of the Indian laws and acts which address various aspects of cybercrimes are as follows:

- Information Technology (Amendment) Act, 2008
- Indian Penal Code 1860
- The Indian Evidence Act 1872
- The Indian Telegraph Act 1885
- Bankers' Book of Evidence Act 1891.

Note: Relevant portions of the ITAA 2008 must be used for registering cases against cybercrime offenses. Investigators are advised to refer to the full acts, for further clarity.

Case study:

Let's take an example case of **Phishing fraud** and understand how details can be captured for registering a case:

Ms. Sowmya is a post graduate in computer application and actively looking for a job online through job portals, classifieds etc., She came across a website called www.my-csjobs.com similar to the popular www.mycsjobs.com website. She registered for a paid service plan through her debit card. She wanted professional resume writing service from the site and didn't get the proper support and response from the site. She then searched about mycsjobs.com on the internet and wrote a mail to the original company about the poor service that they are providing for their customers. The mycsjobs.com customer care representative saw the mail and the attachment having receipt of the payment containing their website logo and their company address in the receipt. The service plan mentioned on the receipt was not offered by them. So, the representative got suspicious and reported it to the management. They contacted Ms. Sowmya and explained the situation in detail and requested the details of the site visited. Ms. Sowmya being tech-savvy, searched in the history of her web browser and found the URL www.my-csjobs.com and sent it to the original company. The MD of mycsjobs.com approached cybercrime police station for filing a complaint against the fake company.

3.2. Penal provisions under IT (Amendment) act 2008

- **66C** – which is chosen for identity theft:
- **66D** – which is chosen for cheating by personation:

As per Information Technology (Amendment) Act, 2008, any cybercrime needs to be investigated by Inspector or above rank officer.

3.3. Information gathered from the Complainant & Intermediaries (Mobile service providers, e-Mail service providers, Webhosting services, ISPs?)

The following details were collected from the intermediaries:

Ms. Sowmya was requested to access her email account with her own credentials, and collect email headers. This can be done by the police officer with the help of the technical expert in front of the complainant.

Indicative Investigation Procedure

- Logs (Registration & Access) details of senders e-mail ID.
- A WHOIS lookup of the domain name mentioned in the URL. In this case, yessbank.com and look for the details where the server is hosted.
- Collect the registrant details, payment details, access logs (IP used for registering a domain name), CP logs.
- Self-attested copies of the same headers should be collected by the IO.
- Also, collect the details of the bank account with which fraud has taken place along with the amount. In this case, fraudulent transaction details.
- Request CDR & SDR of the mobile numbers related to the case.
- After collecting all the details, IO can investigate the case further following the money trail, analyzing the CDR etc.

3.4. Counseling and advice to the victims of cybercrime

Cybercrime can happen to anyone connected to the internet with digital devices. But the victim will never know until there is some incident which has an outcome like loss of reputation, cyber bullying, Posting of morphed images etc. Victims will feel distressed when they are involved in such crimes. They immediately need some support to deal with such incidents.

- It is very important for an investigation officer to stop further victimizing the victim. It's the responsibility of an IO to stop further more damage to the complainant, so they should be extra cautious.
- IO can provide counseling to the victim only after he/she should have a comprehensive understanding of the diversity of the cases reported.
- Damage to the complainant can be controlled by many ways based on the complaints reported:
    - Report the suspected accounts in case of impersonating profiles
    - Take down numbers of the victims from the classified advertisement pages
    - Removal of false information/obscene content from the website
    - Freeze bank accounts, in case the victim transferred the money to the bank for a Job in job scam or matrimonial scam.
    - Block the debit/credit cards etc.

- All these measures can be taken by the investigation officer in consultation with victims.
- All these actions need to be documented properly by the IO with proper evidence and justification.
- There are NGOs which can hear the victim anonymously and counsel the women and children victims.

3.5. Tips to preserve the evidence in most of the cybercrime scenarios

It is vital to preserve the evidence of the case after the charge sheet is filed till is closed.

- Please keep the evidence in a proper packing:
    - If its hard disk, use anti-static covers to avoid any magnetic distortions which may lead to loss of data.
    - If it's a mobile phone, use faraday bags to seize the device, so as the evidence is intact without any modification.
- Document the digital media with tags and barcodes.
- Create a separate inventory list of all the seized media with the case number and other related nomenclature.
- Do not leave the evidence unattended and store them in a cool and dry place.
- Store as a tamper-proof and fireproof package
- Maintain chain of custody and update it regularly if it has to be transferred from one place to another place as part of preservation and analysis.
- Evidence must be legally relevant, so IO should prepare well to submit it to the court of law by adapting to the processes like taking forensic images of the same.

3.6. Institutional setup for cybercrime investigation

A state/UT may be having may be having a designated cybercrime police station/ cyber cells or multiple cybercrime police stations/cyber cells for investigating/assisting cybercrime cases. Since Inspector and above is empowered to investigate cybercrimes cases under the Information Technology (Amendment) Act, 2008. Local police stations may register cybercrime cases and cyber cells/ cybercrime police stations may assist local police in investigations.

3.7. Role of various other stakeholders in the cybercrime investigations

The cybercrime investigations involve multiple stakeholders in investigating cybercrimes. The other investigators involved in the cybercrime investigations are cyber forensic or digital evidence experts.

Internet Service Provider or ISP typically give information on based on the type of request. Most of them are covered below:

- Username of the profile
- Mobile numbers of the user if they are used to register the account
- Other personal details like email ID, address,
- Transactions of the user, how long he is being used the account
- IP address of the user.
- MAC ID- Few ISPs log MAC address or physical address of the device (be cautious it would belong to the access point as well)

Email service provider typically provides information like;

- Username of the email account
- Details of all incoming and outgoing emails along with e-mails stored in a draft folder

- IP address of the account when it was used last time
- IP address of the user when the account was registered
- Date and time of the IP address are given (These are utmost important as most of the IPs are NATed for dynamic usage)
- Secondary email IDs associated with this email and
- User activity for the account with date and time

The mobile service provider typically provide you the data like;

- Customer Application Forms (CAF) Forms — Personal details like name, address. etc.
- Calling number, called number, time, type of call (ISD/STD/Local/SMS, etc.)
- Roaming to other cities, etc.
- Tower locations — Latitude and Longitude of the tower
- Tower data

Social media sites typically provide data like:

- Username of the profile
- Personal details updated in the profile like name, DOB etc. (if available)
- The IP address from where the profile is accessed
- User activity, i.e., date and time of logged in and duration of the active sessions, etc.
- Friends and groups with which the user is associated, etc.
- e-mail ID’s updated in the personal information.

Information typically obtained from financial institutions:

- Personal details updated in the profile of the account holder
- Transactional details
- CAF and other supporting documents submitted by the customer along with the introducer details
- IP address from where the transaction happened in case of Internet banking

Information typically obtained from Website domain owners / hosting providers:

- Registration details
- Access details
- FTP logs
- Payment details
- Technical/administrative/owner of the domain

Information typically obtained from VOIP service providers:

- Registration details
- Access details
- IP addresses
- Payment details
- Called/Calling numbers

CHAPTER-IV

Introduction to social media & Banking frauds

CHAPTER-IV: Introduction to social media & Banking frauds

Social Media enables communication among individuals or communities to create & share content in cyberspace using Internet. Social media is omnipresent & accessible using communication devices like Desktops, smart phones, laptops, Tablets etc. Social media will create a platform for creation and exchange of user generated content. This includes social networking sites, Micro blogging sites, Images & videos sharing sites, Blogs, messengers etc.

After reading this chapter, you would be able to:

- Brief understanding of social media
- Introduction to credit/debit cards
- Identify the pros and cons of social media

Most of the social networking providers have developed their own applications which can be used by the mobile platforms (e.g. Facebook, twitter, LinkedIn, Instagram etc.)

4.1. Types of Social Media

Social media can be widely classified into the following types:

Social networking websites:

They provide a platform for their registered users to connect with other people to share their thoughts & ideas, images and videos. It is also becoming a popular gaming platform where free as well as paid games and apps are available for purchase. Generally, social media users will create a profile for themselves. Social media also supports creation of groups/ communities, create a page for individuals or organizations to promote business, ideas, awareness etc.

Some of the widely used social media sites are:

4.1.1. Facebook

Commonly called FB, is a popular American based free online social media and social networking site. The site supports various regional languages and has the following features.

- Groups - Allows members with similar interests to find each other and interact.
- Pages - Allows members to create and promote a public page.
- Events - Allows members to publicize an event on profiles, groups, pages to invite guests and track who plans to attend.
- Newsfeed: display top trending news and personalized news of users interest

4.1.2. Google+

It is a social networking service owned & operated by Google. Like most of social networking sites it supports sharing photos, status updates, create communities, etc. The unique feature introduced by it is called circles where its users are allowed to group different types of relationships into Circles, text and video chat support through hangouts etc.,

4.1.3. Instagram

It is owned by Facebook and is primarily used as a photo sharing application. It allows users to share their pictures and videos either publicly, or privately with selected followers.

4.1.4. LinkedIn

Online social media networking site aimed for working professionals that allows a person's work profiles and interest to be visible to a wide audience in virtual world.

4.1.5. Pinterest

A mobile application which runs on web browsers also. It is mainly used to share images and GIFs, which began with an idea to share ideas. Users can pin the images and recheck them again.

4.2. Blogs & micro blogs

A blog creates a platform to share descriptive, informal information or thoughts written on a specific interest (e.g. travel, technology, Life experience etc.,) that is published over the internet. The people who write blogs are referred as bloggers. Micro blogging is an online broadcast platform that allows users to create and share short messages, videos, and imagese.g. Twitter, Tumblr, Playtalk, Jaiku etc. The micro-blogging limits the text/message length which acts as a differentiator to traditional blogging.

4.2.1. WordPress

It is a blogging platform that provides free blog hosting for registered users. Registered users can write blogs. Additional services like designing, removing of ads, storage space etc., are offered as a paid service.

4.2.2. Twitter

A micro-blogging site for online news and social networking service. The messages posted by users are called "tweets". There is a word limit of 280 characters for each tweet. Like most others, runs on web browser and supports popular mobile platforms such as android, iOS Windows Phone etc. A hashtag (e.g. #cybercrime) is used to categorize tweets on the basis of topics.

4.3. Online video platform

It is a platform provided by the video hosting service providers where their registered users are allowed to upload video clips, store and play back video on the internet. Some commonly used video service providers are YouTube, MetaCafe, Dailymotion, vimeo etc.

4.3.1. YouTube

It is one of the largest & popular video sharing websites in the world owned by Google. It allows users to upload, view, like, share, add to favourites, subscribe to other users, create a channel, report and comment on videos

4.3.2. Daily motion

It is a video sharing technology platform similar to YouTube.

4.4. Instant Messaging platform

It allows users to exchange messages, images, videos instantly using internet hence the name instant messages. Most of the messengers have their own applications for mobile platforms. The most popular ones are WhatsApp, WeChat, Line, Hike, Telegram, Facebook messenger etc.

4.4.1. WhatsApp

Widely used instant messaging application which also supports Voice over IP (VoIP) that runs on smart phones. It has almost replaced the traditional SMS services. It is supported by most of the phones. It requires a person's mobile number for registration.

4.5. Online drives

It allows users to store photos, videos or any other files online accessible through internet. Some of them provides free online storage for their registered users & are accessible through their own mobile applications. Some of the popular online drive providers are Google Drive, Dropbox, OneDrive, Amazon cloud drive, iCloud Drive etc.

4.5.1. Google Drive

It is a file storage and synchronization service developed by Google. It provides 5TB of free space for its registered users to store their content. Android users can store backup of images, WhatsApp content, contacts, etc. on their drive. It comes pre-installed in android based smart phones

4.5.2. iCloud Drive

It comes pre-packaged with all Apple products. It allows users to store photos, videos, documents, notes, contacts, and more. Users can use their Apple ID or create a new account to use Apple services.

4.6. News Aggregators

The members' posts links, text and images of news aiming to select stories specifically for the internet audience e.g. Reddit, Digg

4.7. Social Bookmarking websites

These are centralized online services which facilitates users to save, add, edit, and share bookmarks or links e.g. Pinboard, ShareThis, Diigo etc.

4.8. Advantages of social media

- **Connectivity:** People can connect from anywhere with anyone to share their thoughts and build relationships. Most of the internet users are active on one or the other social media platforms.
- **Education:** It facilitates to educate from other experts and professionals via the social media. It allows users to follow anyone to learn from them and enhance their knowledge about any field. It allows users to post queries & receive responses from professionals around the world who are knowledgeable in their domain.
- **Newsfeeds/news sharing:** The users share news or current affairs which interests them .People who find those news interesting will share with others and acts as a channel for new information and opinion. Since, large pool of people are active in social media, some media houses only use social media sites for their news sharing.
- **Create awareness**: It is used to create awareness among users on various subjects. Individuals, organizations create their own pages for spreading awareness e.g. awareness pages on cybercrime created by various law enforcement agencies, Traffic awareness, computer basics awareness, cyber security awareness etc.

4.9. Disadvantages of social media

- **Privacy:** Privacy is a major concern for the people on social networking sites. The users are required to provide some personal information such as a full name, e-mail address, date of birth, a phone number, etc. for registering on these social networking sites. Most of the social networking sites offer privacy settings for users to restrict public access of their personal information. However, such data can be misused.

- **Impersonation:** A criminal can create fake account on social networking sites using our name. They can do this by creating another email ID for this purpose. The user can carry out various activities in our name through this fake account.

- **Cyber Bullying:** It is a form of extreme bullying among youth via technology. It is abusive, targeted, deliberate and repeated behaviour that is intended to damage and harm another young person.

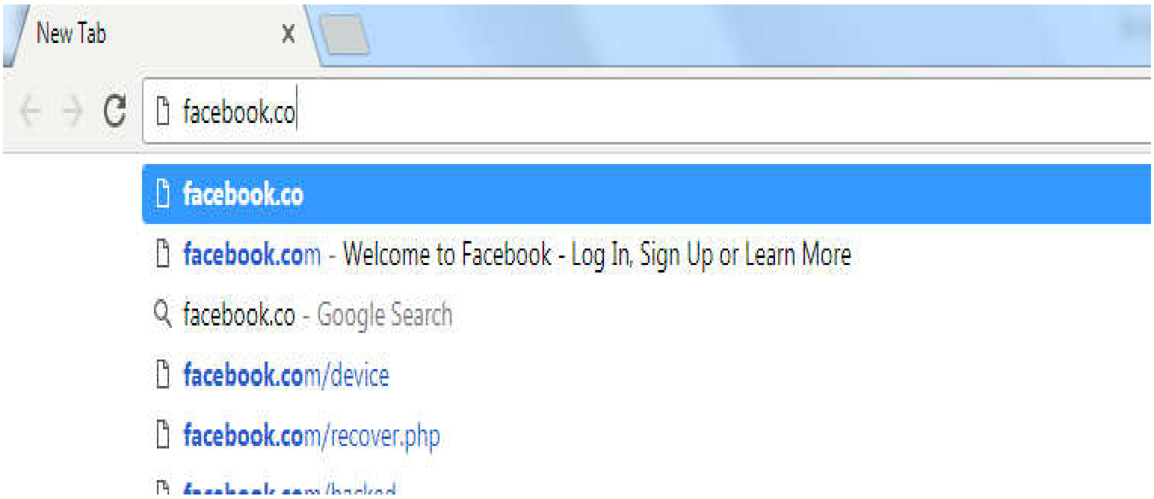
- **Spreading Fake News:** Fake news or Hoax messages spread like wildfire on social media. It may create law and order problem and may end-up causing loss of life in few cases e.g. Boston bombing in 2013, NE exodus in 2012, Muzaffarnagar riots in 2013 etc.,

4.10. Creating Social Media and Messenger Accounts

We have taken up two social media platforms viz. Facebook, Twitter and a messaging platform WhatsApp.

4.10.1. Facebook

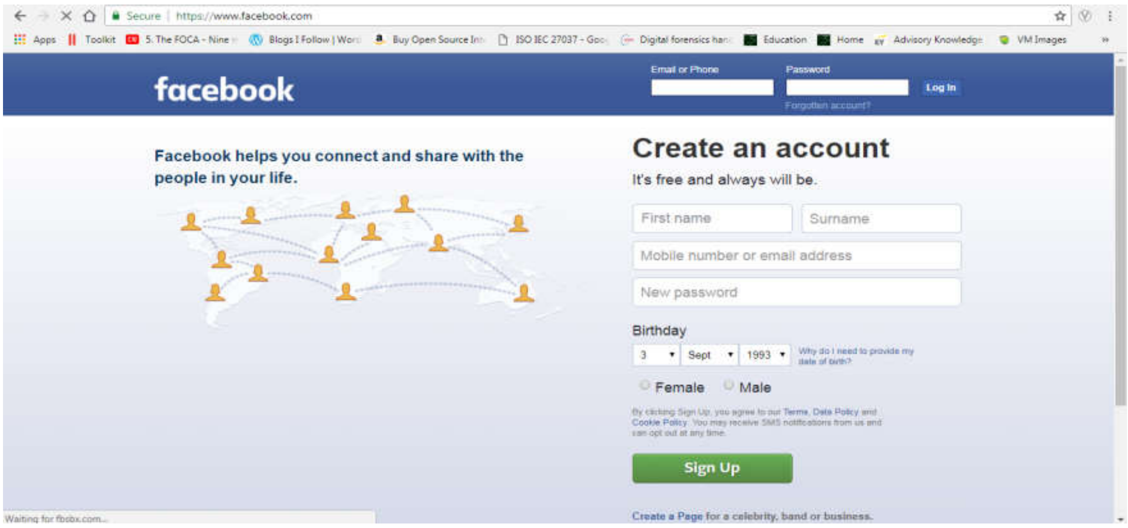
Step I: Browse www.Facebook.com on your web browser.



facebook.co

New Tab
facebook.co
facebook.com - Welcome to Facebook - Log In, Sign Up or Learn More
facebook.co - Google Search
facebook.com/device
facebook.com/recover.php

Step II: Enter your details like first name, last name, mobile number and email address with date of birth and desired password (with minimum 8 characters) to create an account.



https://www.facebook.com

Facebook helps you connect and share with the people in your life.

Create an account

It's free and always will be.

First name | Surname

Mobile number or email address

New password

Birthday: 3 Sept 1993

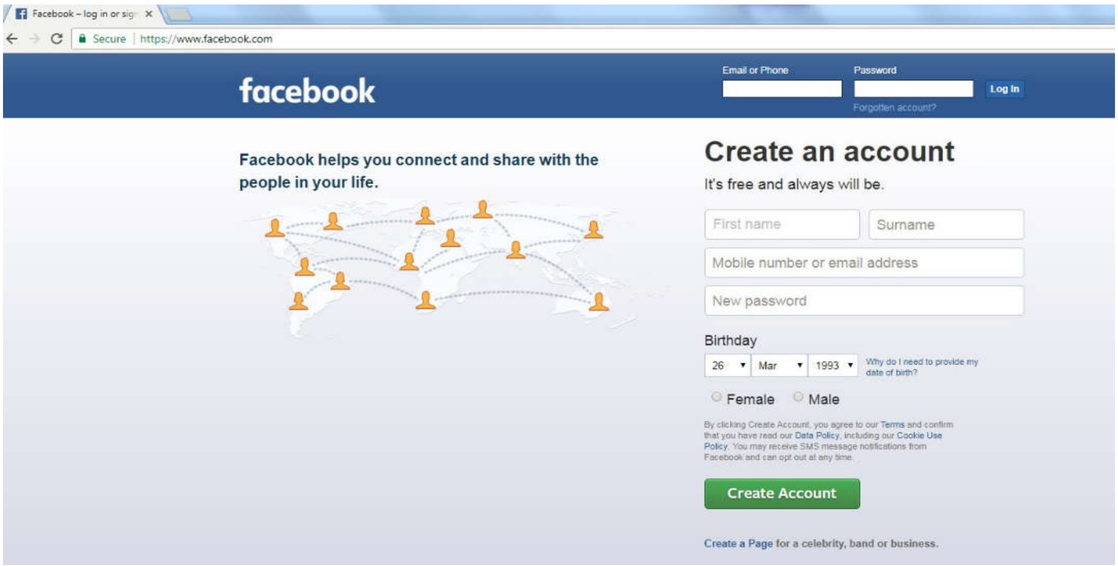
Why do I need to provide my date of birth?

○ Female ○ Male

By clicking Sign Up, you agree to our Terms, Data Policy and Cookie Policy. You may receive SMS notifications from us and can opt out at any time.

Create a Page for a celebrity, band or business.

Step III: Verify your registered e-mail ID



https://www.facebook.com

Facebook helps you connect and share with the people in your life.

Create an account

It's free and always will be.

First name | Surname

Mobile number or email address

New password

Birthday: 26 Mar 1993

Why do I need to provide my date of birth?

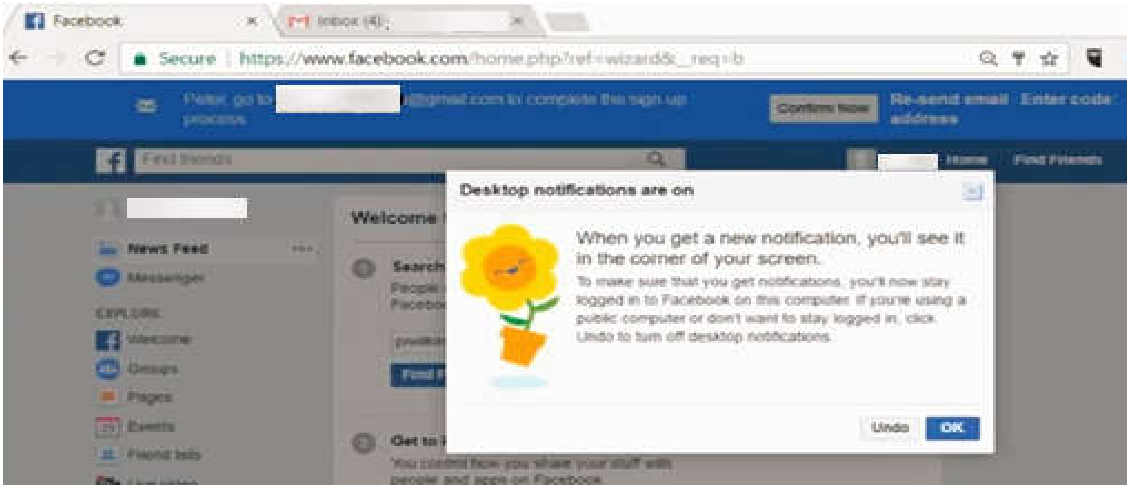
○ Female ○ Male

By clicking Create Account, you agree to our Terms and confirm that you have read our Data Policy, including our Cookie Use Policy. You may receive SMS message notifications from Facebook and can opt out at any time.

Create a Page for a celebrity, band or business.

Step IV: Log in to your e-mail ID and open & copy the confirmation code sent by facebook

`



https://www.facebook.com/home.php?ref=wizard&_rdr

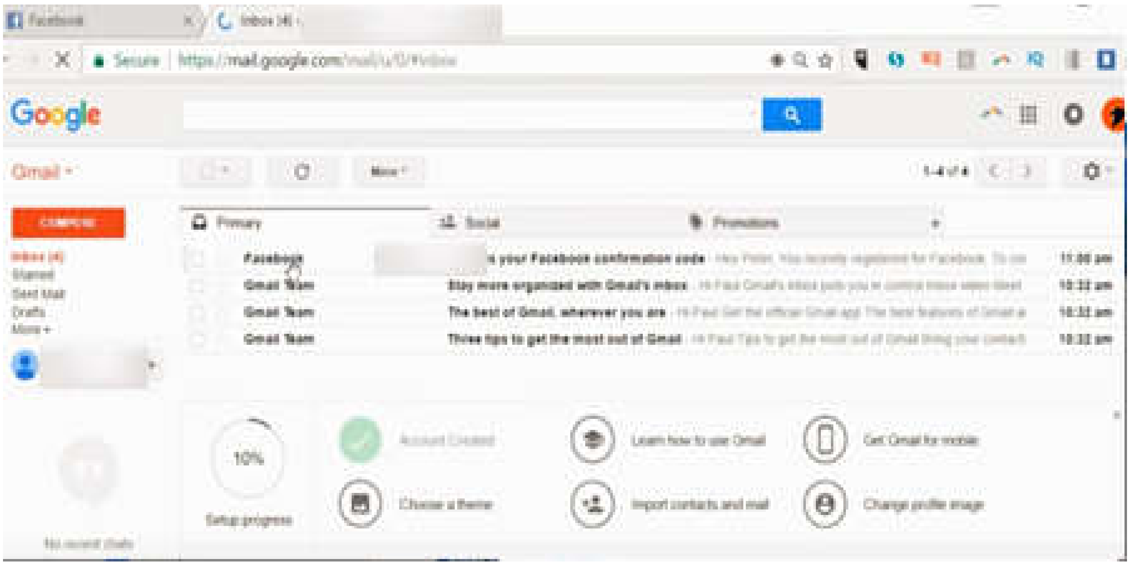
Peter, go to [redacted]@gmail.com to complete the sign up process.

Desktop notifications are on

When you get a new notification, you'll see it in the corner of your screen.

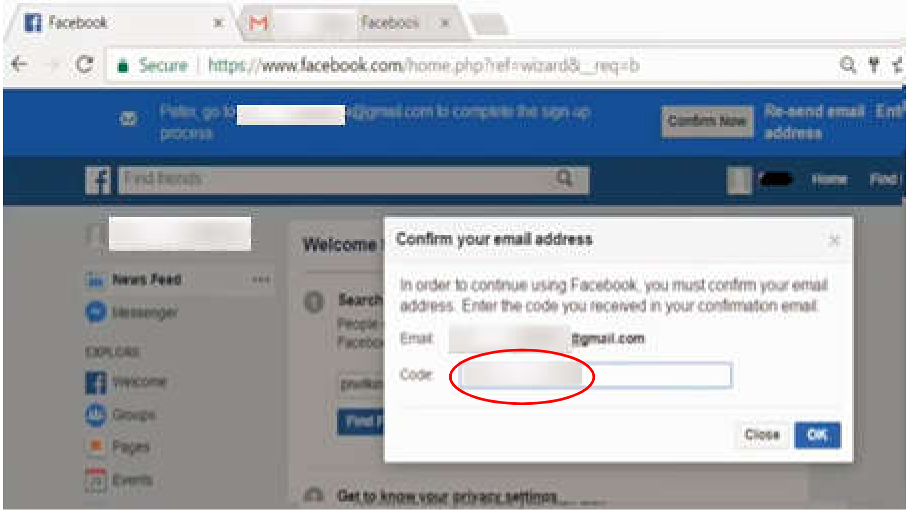
To make sure that you get notifications, you'll now stay logged in to Facebook on this computer. If you're using a public computer or don't want to stay logged in, click Undo to turn off desktop notifications.

You control how you share your stuff with people and apps on Facebook.



Facebook	[redacted] is your Facebook confirmation code	Hey Peter, You recently registered for Facebook. To co	11:00 pm
Gmail Team	Stay more organized with Gmail's inbox	Hi Paul Gmail's inbox puts you in control inbox view direct	10:32 am
Gmail Team	The best of Gmail, wherever you are	Hi Paul Get the official Gmail app. The best features of Gmail a	10:32 am
Gmail Team	Three tips to get the most out of Gmail	Hi Paul Tips to get the most out of Gmail bring your contacts	10:32 am

Step V: Paste the confirmation code copied from your registered e-mail



Peter, go to [redacted]@gmail.com to complete the sign up process

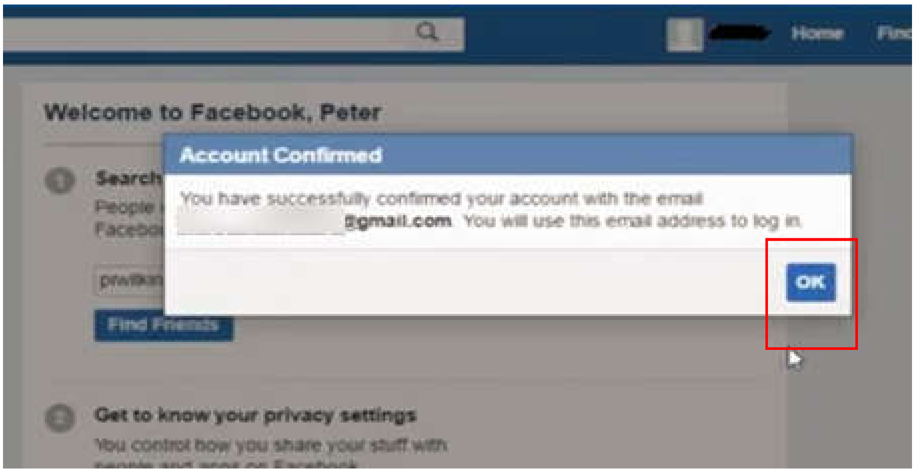
Confirm your email address

In order to continue using Facebook, you must confirm your email address. Enter the code you received in your confirmation email.

Email: [redacted]@gmail.com

Code: [redacted]

Step VI: Click ok to confirm your e-mail address



Welcome to Facebook, Peter

Account Confirmed

You have successfully confirmed your account with the email [redacted]@gmail.com. You will use this email address to log in.

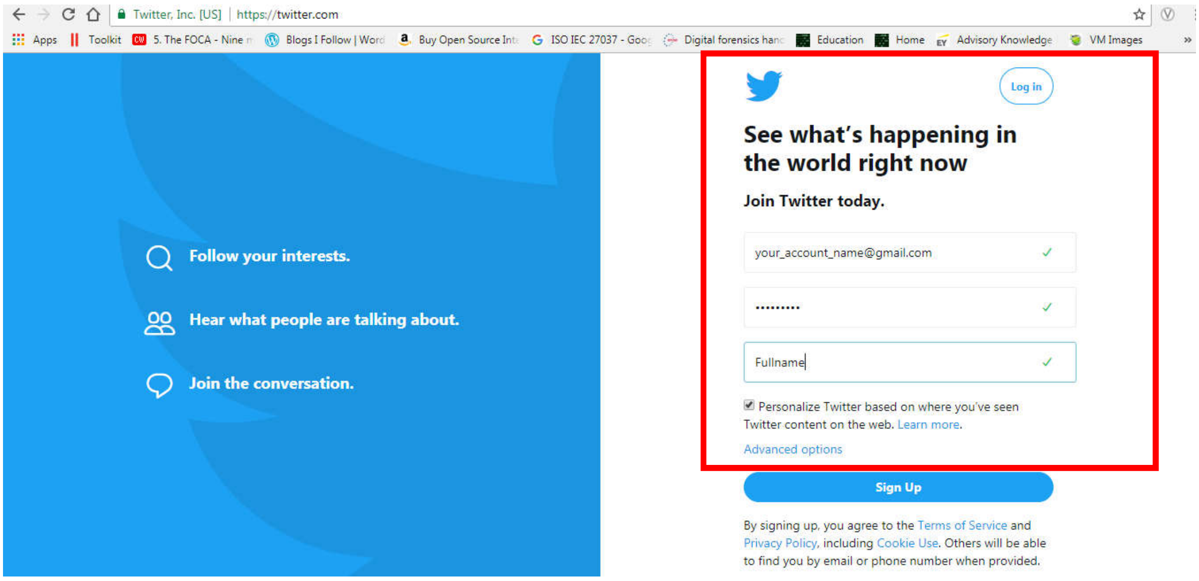
Get to know your privacy settings

You control how you share your stuff with people and apps on Facebook

This completes creation of Facebook account.

4.10.2. Twitter

Step I: Browse www.twitter.com on your web browser. Enter your details like email address, password and full name to display and click on signup.



Follow your interests.

Hear what people are talking about.

Join the conversation.

See what's happening in the world right now

Join Twitter today.

your_account_name@gmail.com ✓

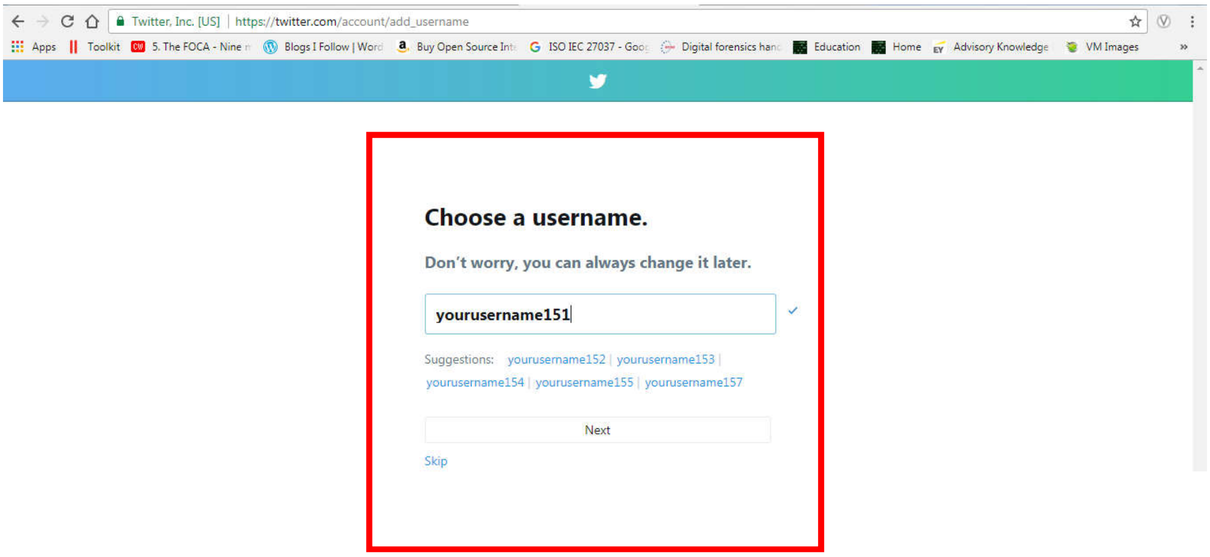
········· ✓

Fullname ✓

☑ Personalize Twitter based on where you've seen Twitter content on the web. Learn more.

By signing up, you agree to the Terms of Service and Privacy Policy, including Cookie Use. Others will be able to find you by email or phone number when provided.

Step-II: Enter desired username for login. It will show you the relative options if it is not available, click next.



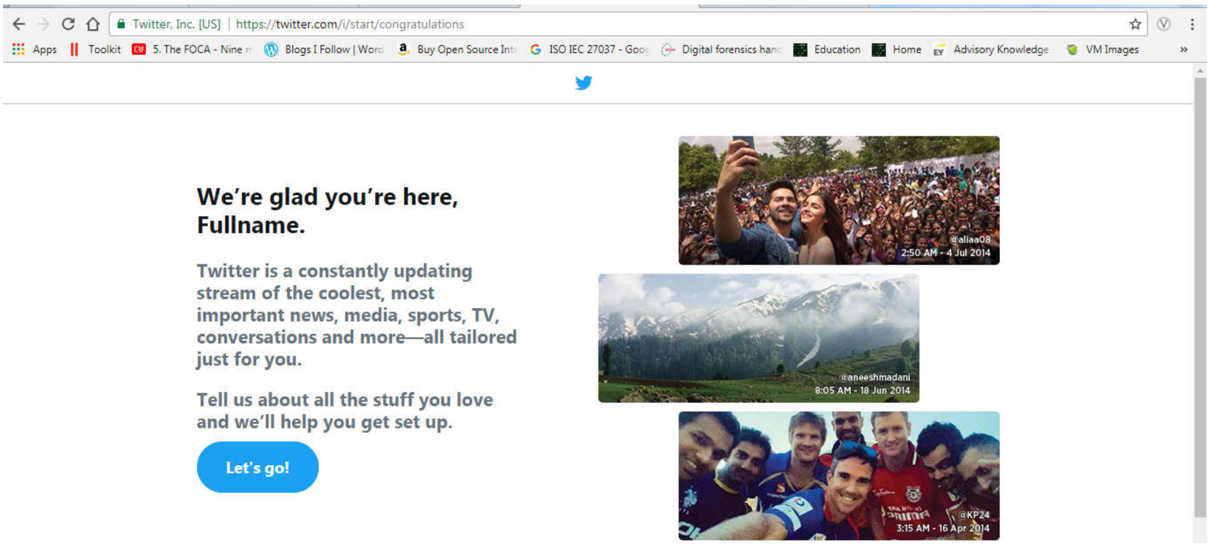
Choose a username.

Don't worry, you can always change it later.

yourusername151 ✓

Suggestions: yourusername152 | yourusername153 | yourusername154 | yourusername155 | yourusername157

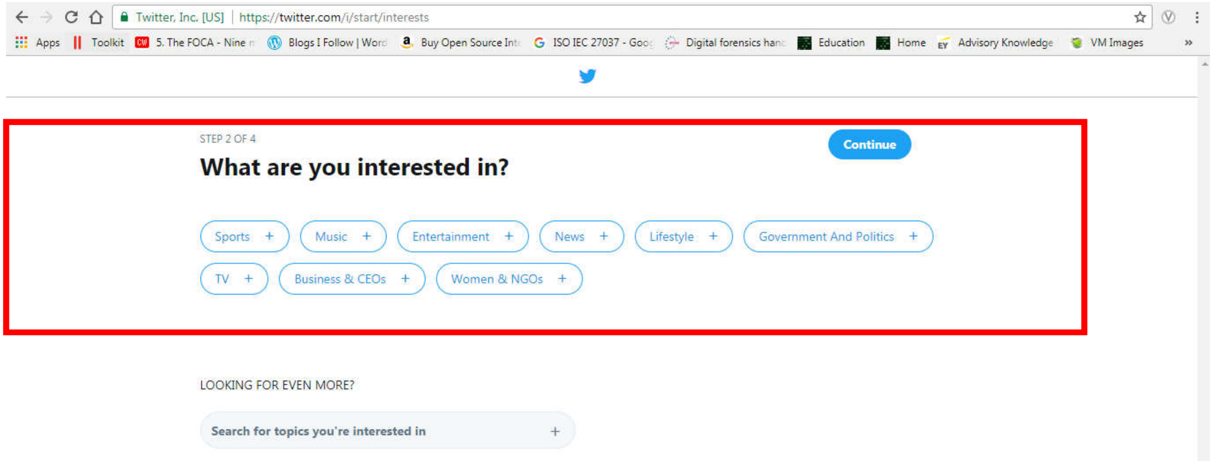
Step-III: Once you enter all the details necessary for signup, it allows you to login into the account by asking certain interests like Music, sports, news, etc.


Twitter, Inc. [US] | https://twitter.com/i/start/congratulations
Apps | Toolkit | 5. The FOCA - Nine | Blogs I Follow | Word | Buy Open Source Int | ISO IEC 27037 - Goog | Digital forensics hand | Education | Home | Advisory Knowledge | VM Images
@aliaa08
2:50 AM - 4 Jul 2014
@aneeshmadani
8:05 AM - 18 Jun 2014
@KP24
3:15 AM - 16 Apr 2014

We're glad you're here, Fullname.

Twitter is a constantly updating stream of the coolest, most important news, media, sports, TV, conversations and more—all tailored just for you.

Tell us about all the stuff you love and we'll help you get set up.

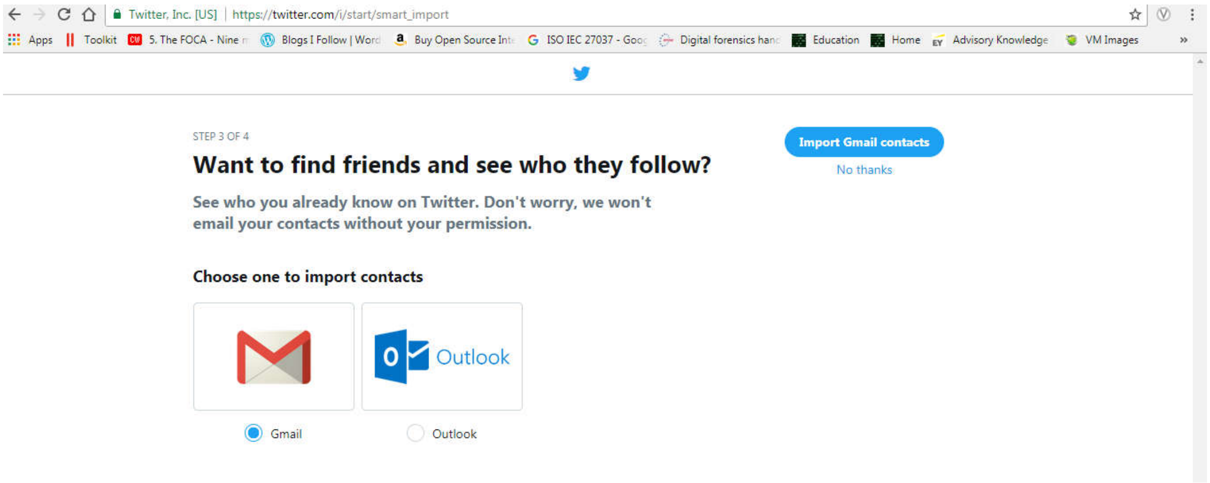

Twitter, Inc. [US] | https://twitter.com/i/start/interests
Apps | Toolkit | 5. The FOCA - Nine | Blogs I Follow | Word | Buy Open Source Int | ISO IEC 27037 - Goog | Digital forensics hand | Education | Home | Advisory Knowledge | VM Images

STEP 2 OF 4

What are you interested in?

Continue
Sports +
Music +
Entertainment +
News +
Lifestyle +
Government And Politics +
TV +
Business & CEOs +
Women & NGOs +
LOOKING FOR EVEN MORE?
Search for topics you're interested in +

Step-IV: Twitter will allow you to import contacts from your mailbox like Gmail or outlook.


Twitter, Inc. [US] | https://twitter.com/i/start/smart_import
Apps | Toolkit | 5. The FOCA - Nine | Blogs I Follow | Word | Buy Open Source Int | ISO IEC 27037 - Goog | Digital forensics hand | Education | Home | Advisory Knowledge | VM Images

STEP 3 OF 4

Want to find friends and see who they follow?

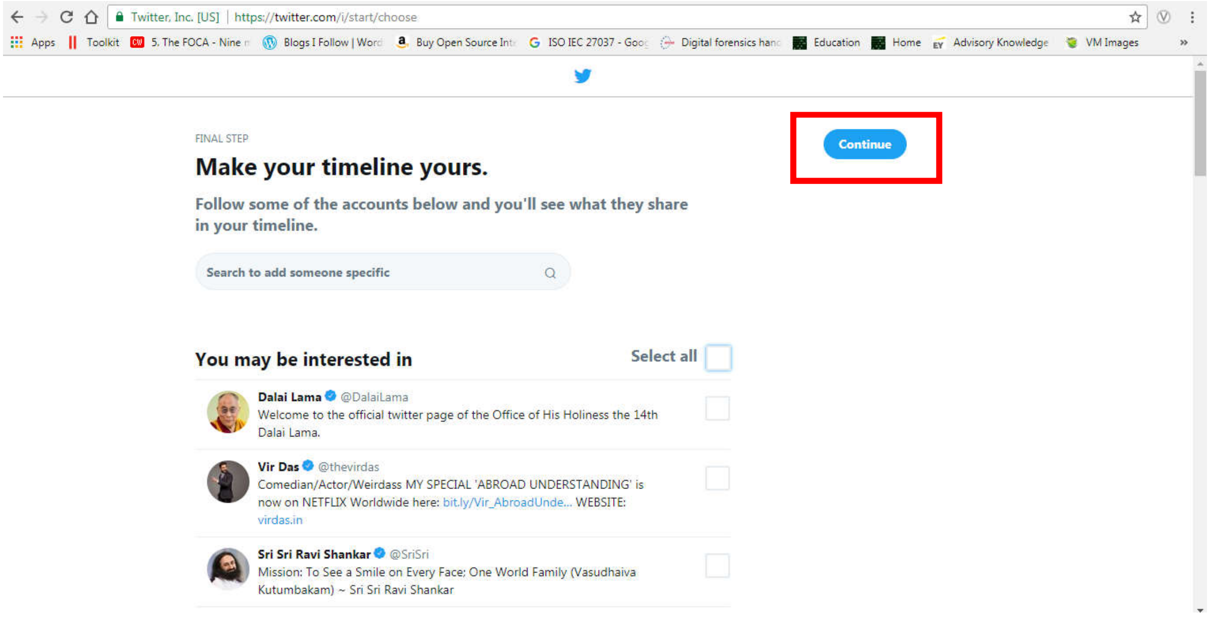
See who you already know on Twitter. Don't worry, we won't email your contacts without your permission.

Choose one to import contacts

● Gmail ○ Outlook

Import Gmail contacts
No thanks
Outlook

Step-V: After successful login and twitter will suggest some profiles to follow. Click on continue, You can share your own text messages using –"What's happening" box and you can "follow" for "tweets" from many individuals and groups.



FINAL STEP

Make your timeline yours.

Follow some of the accounts below and you'll see what they share in your timeline.

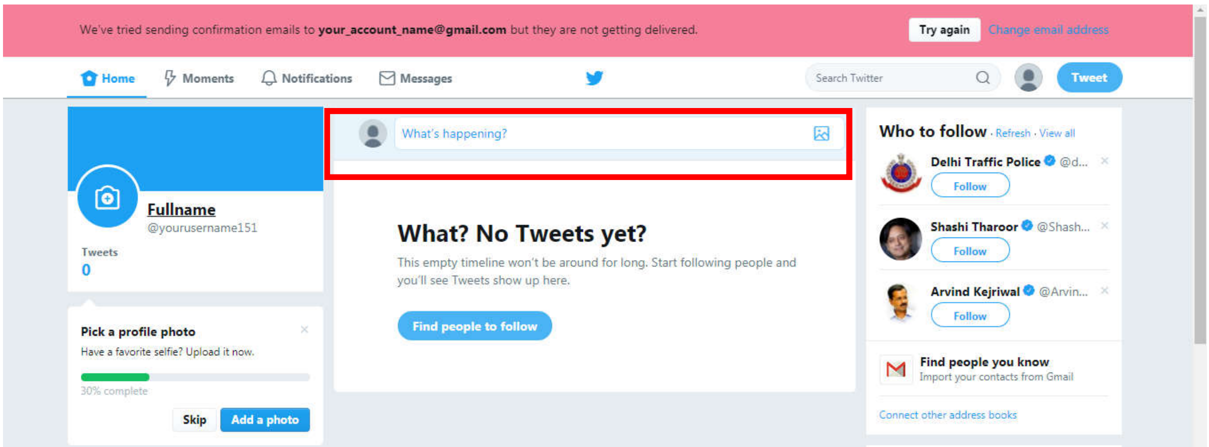
Search to add someone specific

You may be interested in — Select all □

Dalai Lama @DalaiLama
Welcome to the official twitter page of the Office of His Holiness the 14th Dalai Lama. □

Vir Das @thevirdas
Comedian/Actor/Weirdass MY SPECIAL 'ABROAD UNDERSTANDING' is now on NETFLIX Worldwide here: bit.ly/Vir_AbroadUnde... WEBSITE: virdas.in □

Sri Sri Ravi Shankar @SriSri
Mission: To See a Smile on Every Face: One World Family (Vasudhaiva Kutumbakam) ~ Sri Sri Ravi Shankar □



We've tried sending confirmation emails to **your_account_name@gmail.com** but they are not getting delivered.

Fullname
@yourusername151
Tweets
0

Pick a profile photo
Have a favorite selfie? Upload it now.
30% complete

What? No Tweets yet?

This empty timeline won't be around for long. Start following people and you'll see Tweets show up here.

Who to follow · Refresh · View all

Delhi Traffic Police @d...

Shashi Tharoor @Shash...

Arvind Kejriwal @Arvin...

Find people you know
Import your contacts from Gmail

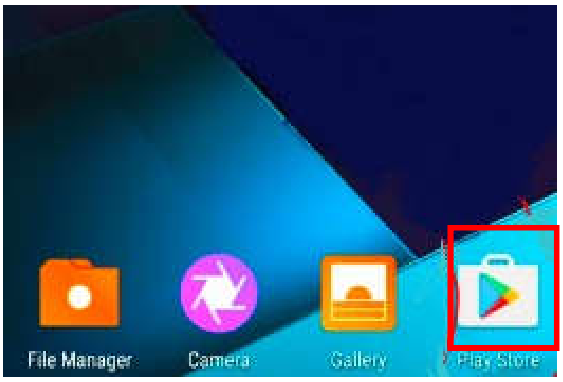
Connect other address books

4.10.3. WhatsApp

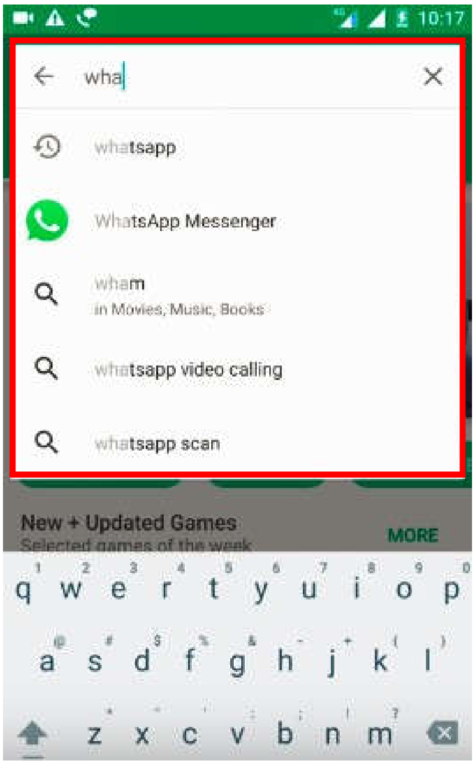
Installing WhatsApp is very simple. You can download and it on your phone from Play Store (Google) and App Store (Apple). This can be used by registering on the app through your valid mobile number.

The steps below explains the process of downloading and installing WhatsApp on android platform

Step I: Select the icon (given in the image below) on your phone for opening the play store app



Step II: Type WhatsApp in the search bar.


wha

whatsapp

WhatsApp Messenger

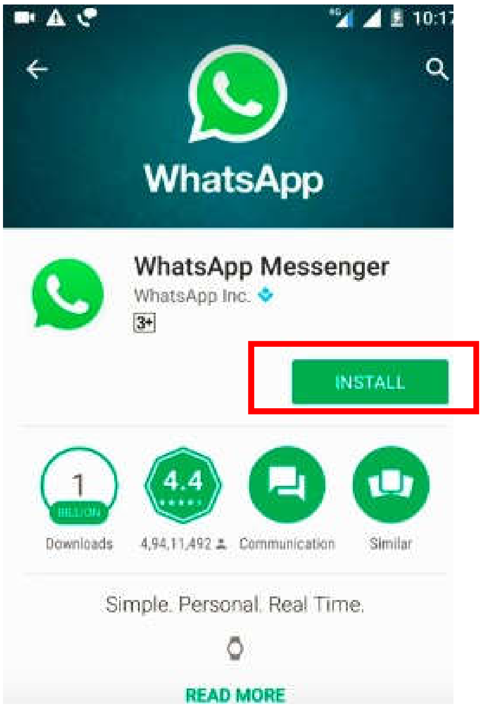
wham
in Movies, Music, Books

whatsapp video calling

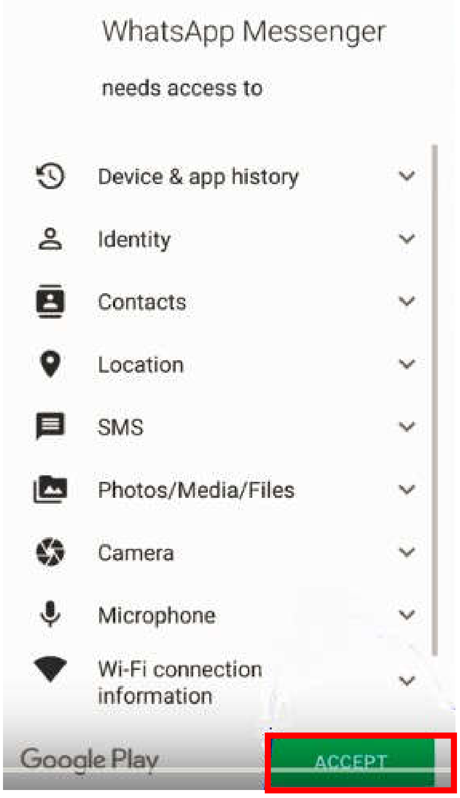
whatsapp scan

New + Updated Games
Selected games of the week

Step III: Click on Install



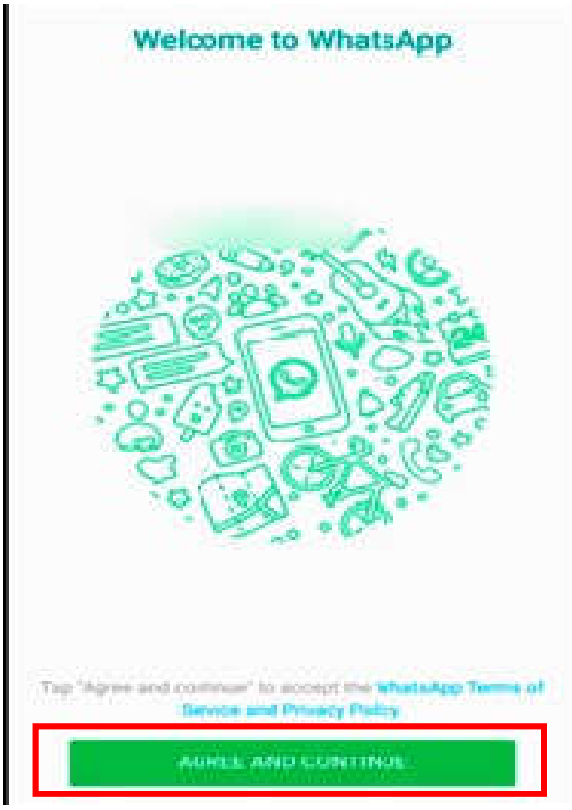
Step IV: Select & restrict access based on your requirement



WhatsApp Messenger

needs access to

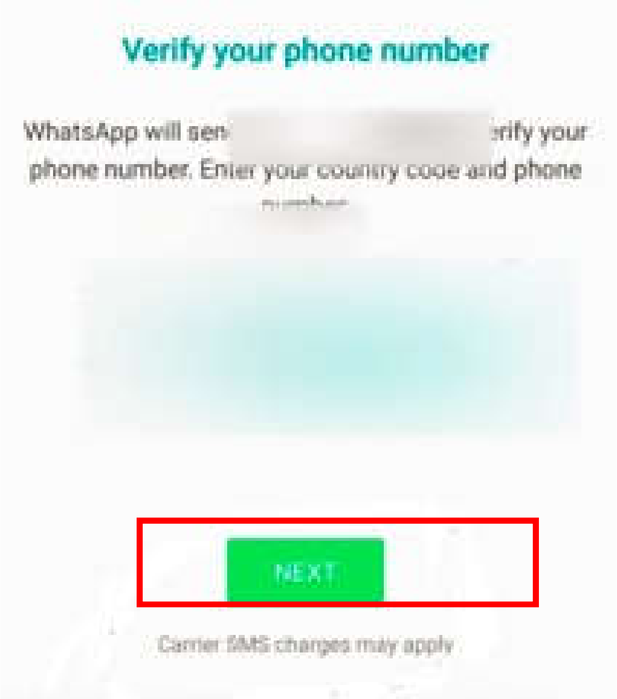
Step V: Read the terms of service and privacy policy. Click on agree and continue



Welcome to WhatsApp

Tap "Agree and continue" to accept the WhatsApp Terms of Service and Privacy Policy

Step VI: Verify your account by entering your valid mobile number

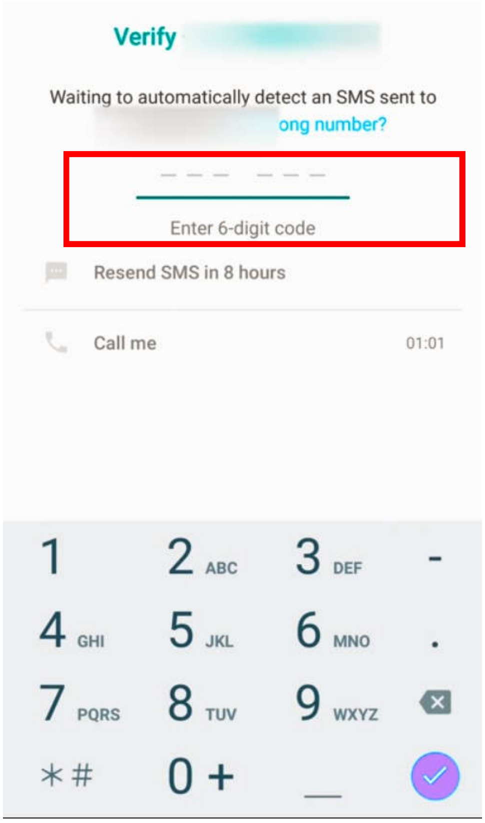


Verify your phone number

WhatsApp will sen [illegible] erify your phone number. Enter your country code and phone number.

Carrier SMS charges may apply

Step VII: Enter the code received by WhatsApp through SMS



Verify [redacted]

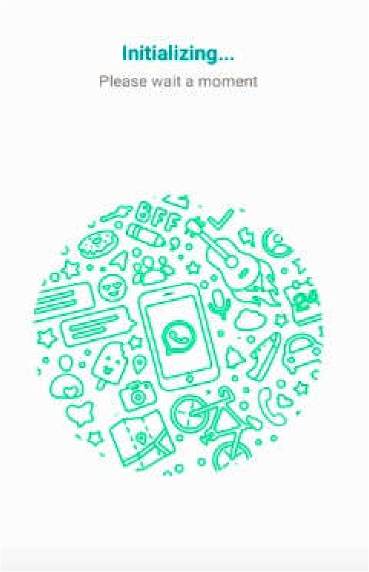
Waiting to automatically detect an SMS sent to [redacted] ong number?

Enter 6-digit code

Resend SMS in 8 hours

Call me 01:01

Step VIII: Start using the Application.



Initializing...

Please wait a moment

4.11. Exercises

1. Create a Facebook account and identify a URL of the any of your friends account. Also, create a Facebook group and share messages among yourselves.
2. Install WhatsApp on the phone and send messages, Image, videos etc., Delete contents shared earlier. Create a WhatsApp group and share contents e.g. messages, Images, Videos
3. Create a twitter account and tweet any cybercrime awareness message. Follow your friends, your official twitter account (If available). Retweet any cybercrime awareness messages.

4.12. Introduction to types of cards in Financial Transactions

Cards can be classified on the basis of their issuance, usage and payment by the card holder. There are three types of cards

- Debit cards
- Credit cards and
- Prepaid cards

4.12.1. Debit Card

It is a plastic card that enables the card holder to access his / her bank account electronically.

- Uses: Withdraw funds, make purchase.
- It is connected to card holder's savings or current account and hence known as a Checking Card.
- Akin to an electronic cheque book, balance is essential to use debit card.
- If the withdrawal request or payment request cannot be met by bank balance then transaction fails.
- Most of the banks provide debit cards when bank account is created and does not ask credit worthiness.

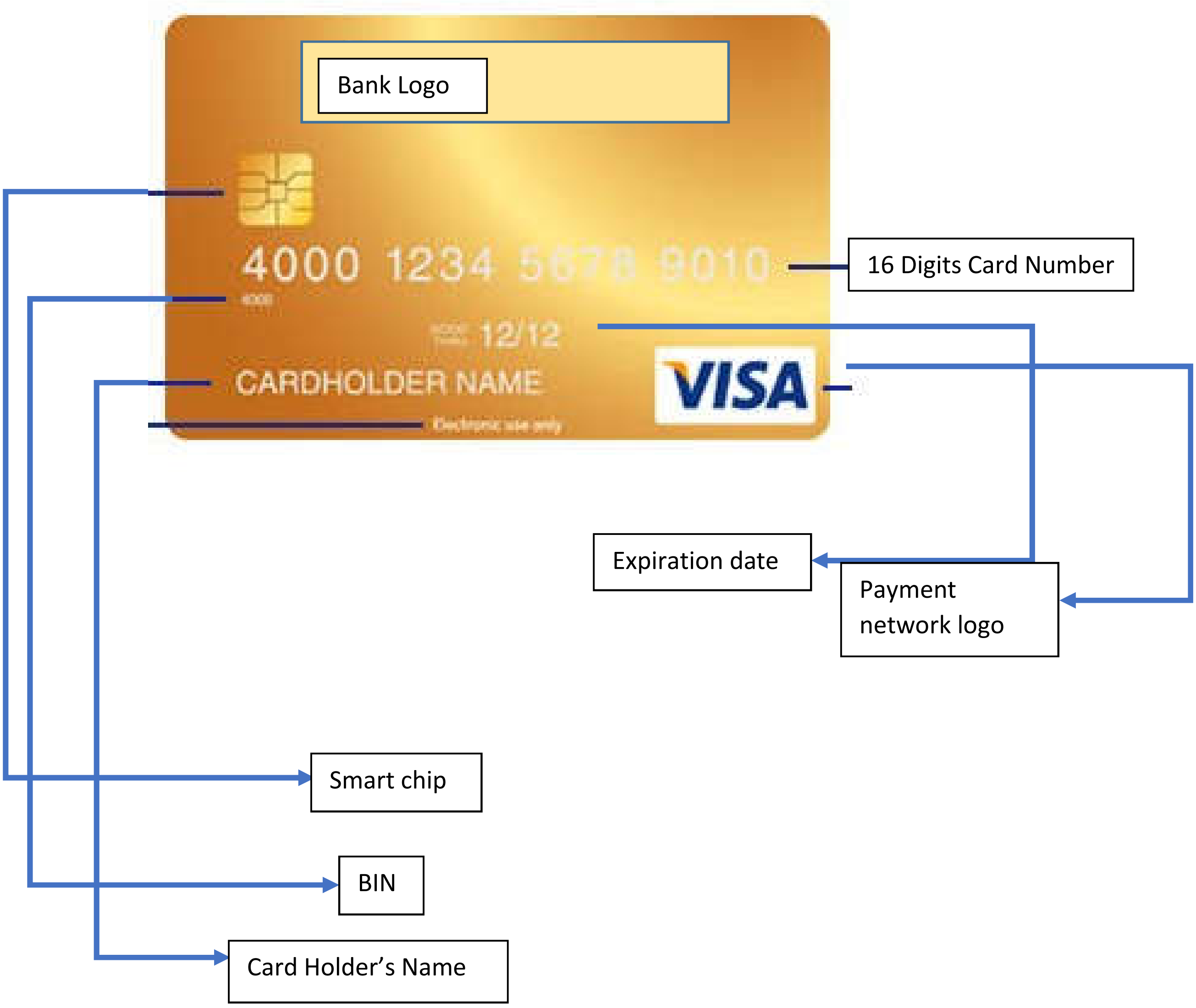
4.12.2. Credit Card

Like debit card, credit card is also a plastic card that enables the card holder to access his / her bank account electronically. However, unlike deb[redacted]it card is not directly linked to bank account but to the bank or financial institution which has issued it.

- Uses: Withdraw funds, make purchase.
- It creates a revolving account from which cardholder can borrow money for withdrawal and payments.
- Since it is not directly linked to bank account and works on the principle of credit, it comes with a credit limit and the amount of money utilised has to be repaid within stipulated time frame.
- Like loans, late payment fee is charged with high interest. Thus, credit worthiness is important in obtaining a credit card unlike debit card.
- The limit of usage depends on the balance in linked account and credit line may increase or decrease. This depends on cardholder's creditworthiness which is set by the card issuer.

4.12.3. Parts of a Debit or Credit Card

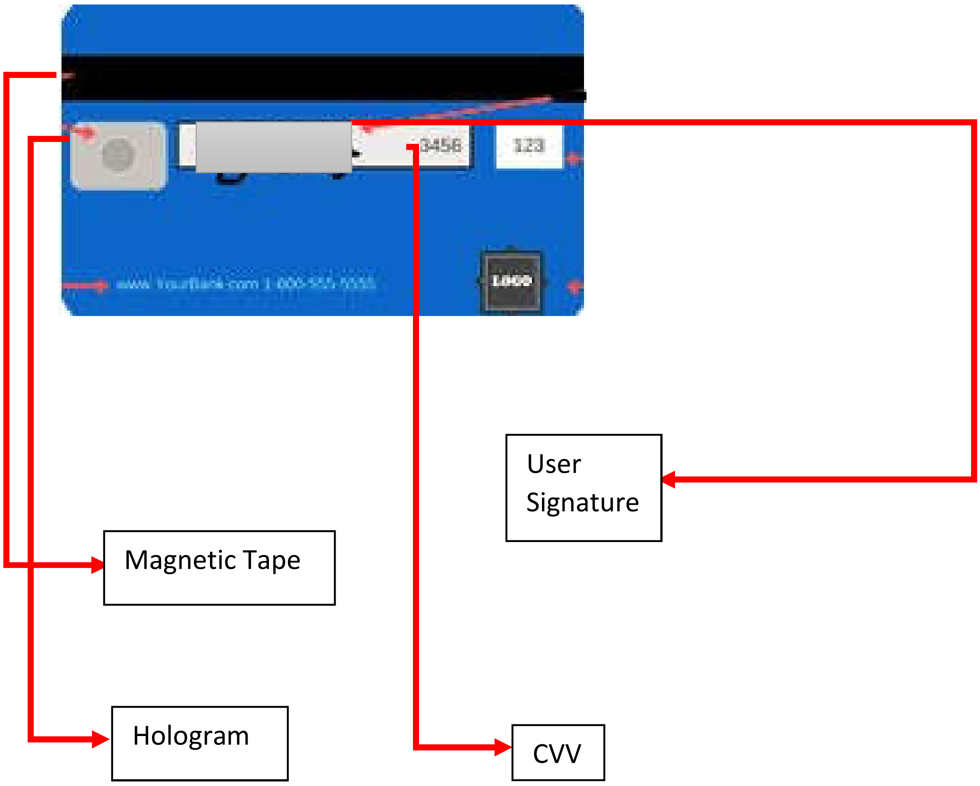
Front Side



Description:

- Issuer/Bank Logo: This is the financial institution or the bank that has issued the card
- Smart Chip: Additional feature to the magnetic-stripe which is at the back.
- BIN: The first 4 or 6 digits of a payment card number (credit cards, debit cards, etc.) are known as Bank Identification Number (BIN).
- Card Holder's Name: Name of the card holder which is the same as the bank account holder's name to which it is linked
- Card Number: 16 digit card number linked to bank account. One of the most critical information.
- Expiration Date: Month of expiry
- Payment network logo: It is the type of card. The cards commonly used are Maestro, MasterCard, Visa, Rupay and American Express. .

Back Side of Card



Description:

- **Magnetic Tape**: The black strip contains information about user and the card. It can be read by specialized devices known as card readers
- **Hologram:** A three-dimensional image which is a security feature and helps merchants identify authenticity of the card.
- **User Signature**: Signature of the card holder.
- **CVV**: Card Verification Value or CVV is a security feature and must not be shared with anyone. It is often a three-digit code on the back of the card and is preceded by last four digits of the card number.

Card Skimming: It is a type of credit/debit card theft where criminals use a small device (Skimmer) to illegally copy the information from the magnetic strip in an otherwise legitimate credit or debit card transactions.

Skimming commonly occurs at retail outlets, bars, restaurants, petrol stations and at ATM's fitted with a skimming device.

Note: A Skimmer is a device which is used to capture and store the data from the magnetic stripe of a card.

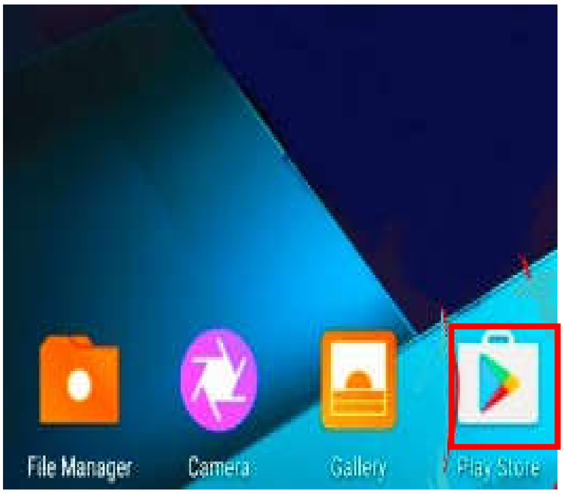
Criminals also call victims impersonating as bank officials and mention that your card will be blocked and to avoid the same request card number, expiry date, Card Verification Value (CVV) number. They also deceive victims to share One Time Password (OTP) received on phone by mentioning security code, reset code etc. Fearing of blocking of the card, victims reveal card details resulting in losing their money.

Awareness:

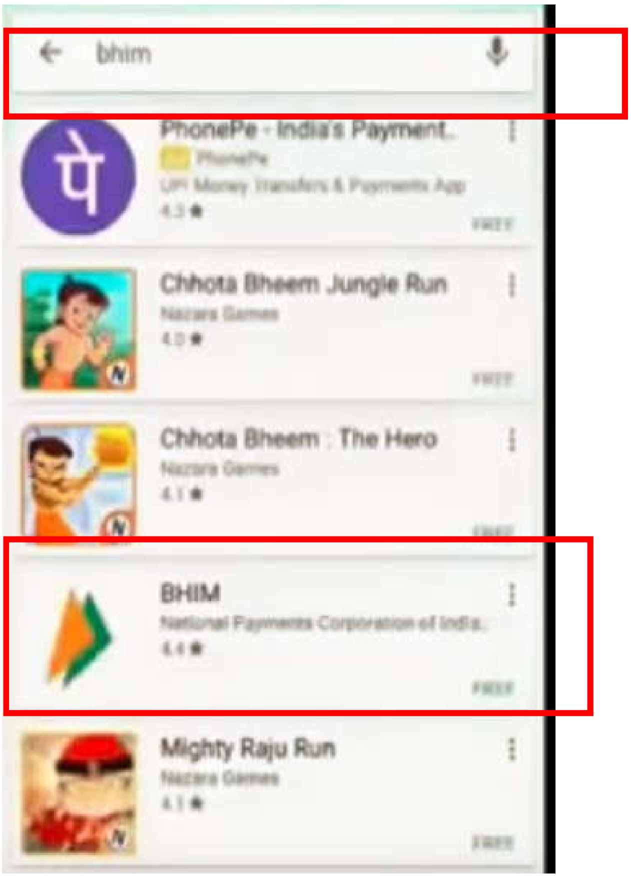
- Cover the keypad with you other hand while typing your PIN.
- Change your PIN frequently and avoid using mobile numbers, date of birth etc., as PIN.
- Look for Hidden Cameras in ATM's & Check the Keypad for key loggers (keypad overlays).
- Inspect the ATMs & watch for signs of tampering, such as new scratches, discolored keys, flashing lights and visible wires.
- Using ATMs located inside / outside bank branches is also safer due to the increased security compared to ATMs on the street.
- Report to the bank right away if you notice withdrawals or purchases that you didn't make.
- Never share your OTP, PIN, and CVV with anyone.

How to install and use BHIM App:

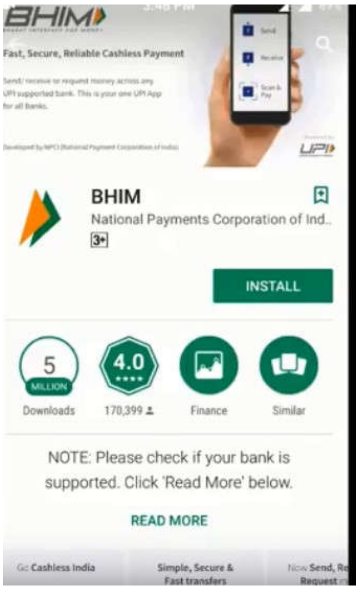
Step I: Select the icon (given in the image below) on your phone for opening the play store app.



Step II: Search for Bhim in the search bar

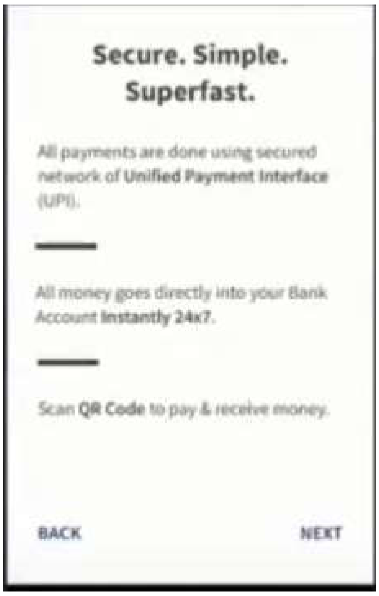


Step III: Install BHIM



NOTE: Please check if your bank is supported. Click 'Read More' below.

Step IV: Click Next



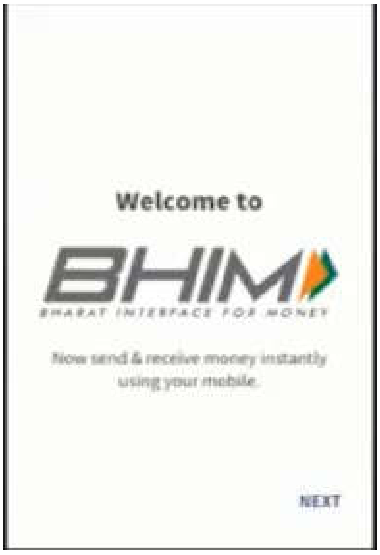
Secure. Simple. Superfast.

All payments are done using secured network of Unified Payment Interface (UPI).

All money goes directly into your Bank Account Instantly 24x7.

Scan QR Code to pay & receive money.

Step V: Click Next



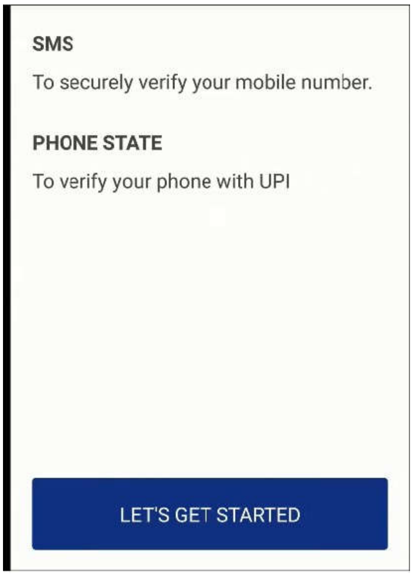
Welcome to

BHIM

BHARAT INTERFACE FOR MONEY

Now send & receive money instantly using your mobile.

Step VI: Click on Let's get Started



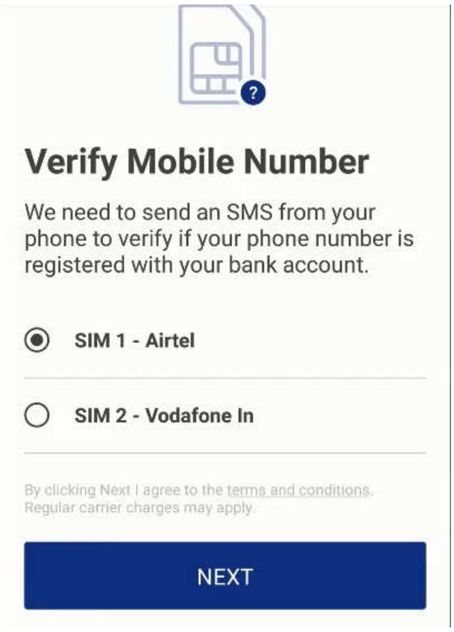
SMS

To securely verify your mobile number.

PHONE STATE

To verify your phone with UPI

Step VII: Select mobile number registered with your bank account



Verify Mobile Number

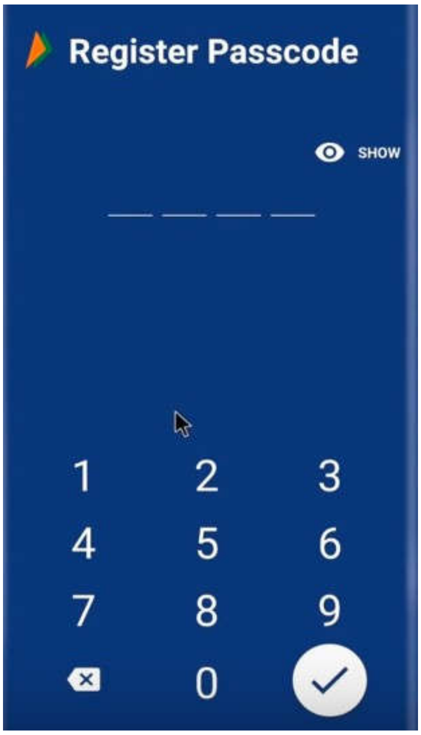
We need to send an SMS from your phone to verify if your phone number is registered with your bank account.

● SIM 1 - Airtel

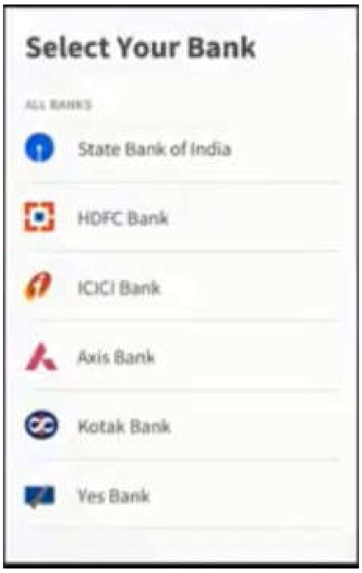
○ SIM 2 - Vodafone In

By clicking Next I agree to the terms and conditions.
Regular carrier charges may apply.

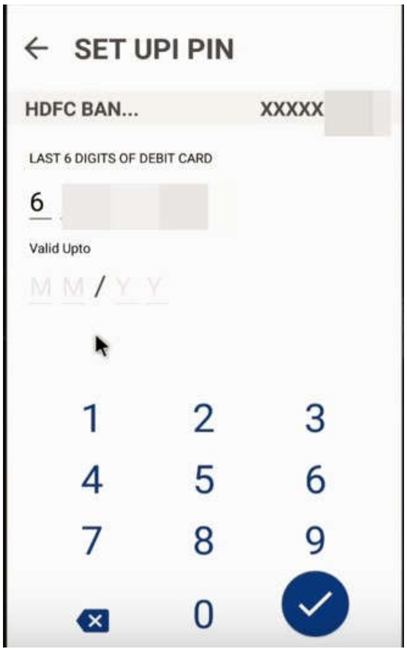
Step VIII: Create password that you will need to enter each time you try to log into the app.



Step IX: Select your bank



Step X: Set UPI PIN which will be used before making transaction



SET UPI PIN

HDFC BAN... XXXXX

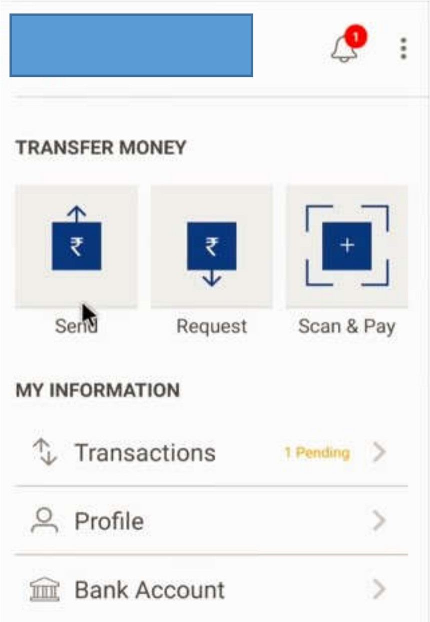
LAST 6 DIGITS OF DEBIT CARD

6

Valid Upto

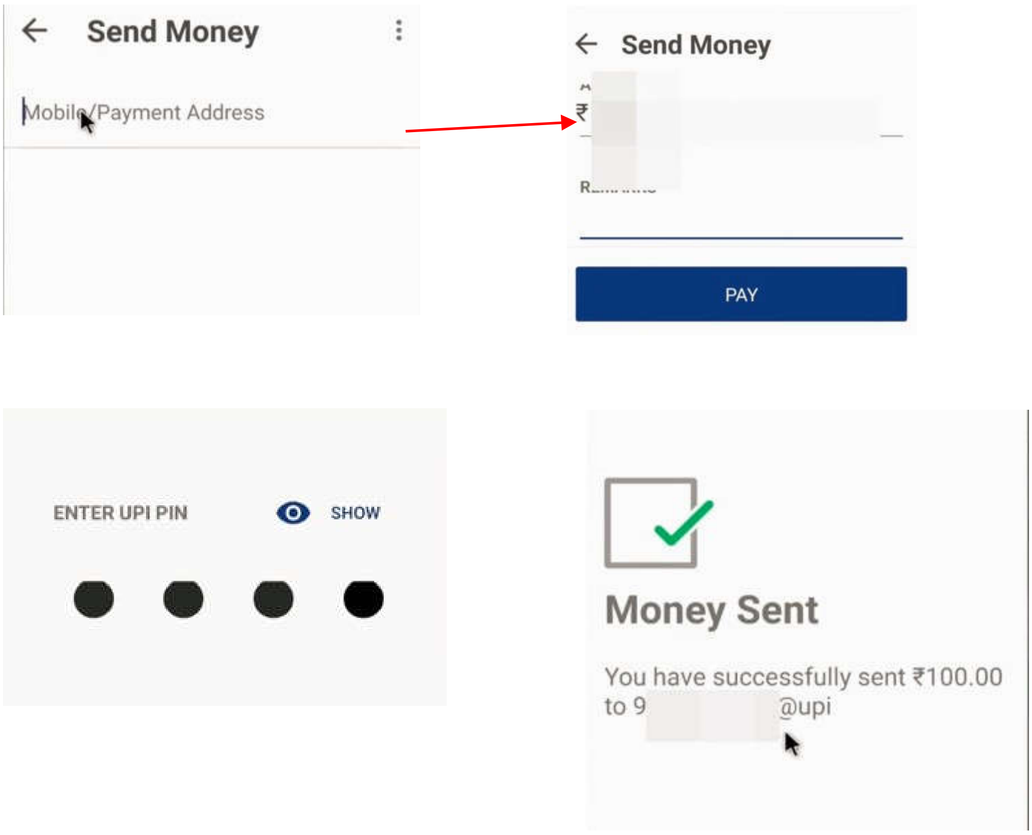
M M / Y Y

Step XI: We are now ready to transact using the app.

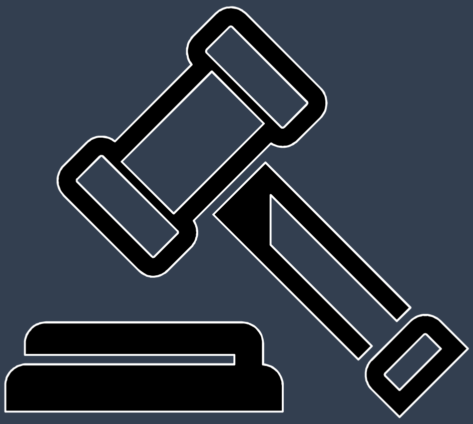


[redacted]

Step XII: Money sent through UPI



You have successfully sent ₹100.00 to 9 @upi



CHAPTER-V

Cyber Laws

CHAPTER-V: Cyber Laws

Why should you read this Chapter?

As our world changes and development in technology gets doubled up every year, there is always a possibility of crime happening online. Individuals and organisations are desperate to get help and protected against such heinous crimes. Law enforcement should be competent enough to face such dreadful wrong doings and the technology being used by them.

After reading this book, you would be

- Identify various crimes with which law enforcement is dealing presently.
- Familiarize yourself with law related to cyber and legal aspects to curb them.

It is important to understand both law and technology being a police officer. So as this book also focuses on the said two aspects. Many of the sections you find in this manual are not comprehensively illustrated, to keep it more precise and reasonable. Mostly, it was only the gist of each element was selected and presented the same.

5.1. Introduction to Information Technology (IT) ACT

- UN General Assembly enacted Model Law adopted by United Nations Commission on International Trade Law (UNICITRAL) by the resolution A/RES/51/162, dated 30 January 1997
- Then India passed the Information Technology ACT 2000 in May 2000 and came in to effectiveness on 17th October 2000
- This Information Technology Act is amended substantially through Information Technology Amendment Act 2008 which was passed by both the houses on 23 & 24 December 2008.
- This act got presidential assent on 5th Feb 2009 and came in to effectiveness on 27th October 2009.

Essence of information technology (IT) ACT:

1. IT Act 2000 addressed the following issues
   a. Legal Recognition of Electronic Documents
   b. Legal Recognition of Digital Signatures
   c. Offenses and Contraventions
   d. Justice Dispensation Systems for Cybercrimes
2. ITAA, 2008 is often referred as the enhanced version of IT Act 2000 as it additionally focused on Information Security.
3. Several new sections on offences like Cyber Terrorism, Data Protection were added in ITAA, 2008.

5.2. Important sections under IT Act for discussion

5.2.1. Section 43: Penalty and Compensation for damage to computer, computer system, etc.

If any person without permission of the owner or any other person who is in-charge of a computer, computer system or computer network –

(a) Accesses or secures access to such computer, computer system or computer network or computer resource

(b) downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;

(c) Introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;

(d) damages or causes to be damaged any computer, computer system or computer network, data, computer data base or any other programmes residing in such computer, computer system or computer network;

(e) Disrupts or causes disruption of any computer, computer system or computer network;

(f) Denies or causes the denial of access to any person authorized to access any computer, computer system or computer network by any means;

(g) provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made there under,

(h) Charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network,

(i) Destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means (Inserted vide ITAA-2008)

(j) Steals, conceals, destroys or alters or causes any person to steal, conceal, destroy or alter any computer source code used for a computer resource with an intention to cause damage, he shall be liable to pay damages by way of compensation to the person so affected.

5.2.2. Section 66 Computer Related Offences

If any person, dishonestly, or fraudulently, does any act referred to in section 43, he shall be *punishable with imprisonment for a term which may extend to three years or with fine which may extend to five lakh rupees or with both.*

5.2.3. Section 66 B Punishment for dishonestly receiving stolen computer resource or communication device

Whoever dishonestly receives or retains any stolen computer resource or communication device knowing or having reason to believe the same to be stolen computer resource or communication device, shall be *punished with imprisonment of either description for a term which may extend to three years or with fine which may extend to rupees one lakh or with both.*

5.2.4. Section 66C Punishment for identity theft

Whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, shall be *punished with imprisonment* *of either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh.*

5.2.5. Section 66D Punishment for cheating by personation by using computer resource

Whoever, by means of any communication device or computer resource cheats by personation, shall be *punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees.*

Note: Section 66D is also called as 419 scam or advanced fee scam. The number "419" refers to the section of the Nigerian Criminal Code dealing with fraud. Most of the cheating by personation frauds like fake cheques, foreign money transfers, fake e-mailers, anonymous friend scams, phishing scams comes under this category.

5.2.6. Section 66E Punishment for violation of privacy

Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be *punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both.*

5.2.7. Section 66F Punishment for cyber terrorism

(1) Whoever, - (A) with intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people by –

(i) Denying or cause the denial of access to any person authorized to access computer resource; or

(ii) Attempting to penetrate or access a computer resource without authorisation or exceeding authorized access; or

(iii) introducing or causing to introduce any Computer Contaminant and by means of such conduct causes or is likely to cause death or injuries to persons or damage to or destruction of property or disrupts or knowing that it is likely to cause damage or disruption of supplies or services essential to the life of the community or adversely affect the critical information infrastructure specified under section 70, or

(B) knowingly or intentionally penetrates or accesses a computer resource without authorization or exceeding authorized access, and by means of such conduct obtains access to information, data or computer database that is restricted for reasons of the security of the State or foreign relations; or any restricted information, data or computer database, with reasons to believe that such information, data or computer database so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise, commits the offence of cyber terrorism.

(2) Whoever commits or conspires to commit cyber terrorism shall be punishable with imprisonment which may extend to imprisonment for life.

Section 67 provides for punishment to whoever transmits or publishes or causes to be published or transmitted, any material which is obscene in electronic form with imprisonment for a term which may extend to five years and with fine which may extend to Rs.1 lakh on first conviction. In the event of second or subsequent conviction the imprisonment would be for a term which may extend to ten years and fine which may extend to Rs. 2 lakhs. As per ITAA 2008, Section 67 is given as under:

5.2.8. Section 67 Punishment for publishing or transmitting obscene material in electronic form

Whoever publishes or transmits or causes to be published in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be *punished on first conviction with imprisonment of either description for a term which may extend to three years and with fine which may extend to five lakh rupees and in the event of a second or subsequent conviction with imprisonment of either description for a term which may extend to five years and also with fine which may extend to ten lakh rupees.*

5.2.9. Section 67 A Punishment for publishing or transmitting of material containing sexually explicit act, etc. in electronic form

Whoever publishes or transmits or causes to be published or transmitted in the electronic form any material which contains sexually explicit act or conduct shall be *punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees.*

5.2.10. Section 67 B Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form

Whoever,-

(a) Publishes or transmits or causes to be published or transmitted material in any electronic form which depicts children engaged in sexually explicit act or conduct or

(b) creates text or digital images, collects, seeks, browses, downloads, advertises, promotes, exchanges or distributes material in any electronic form depicting children in obscene or indecent or sexually explicit manner or

(c) Cultivates, entices or induces children to online relationship with one or more children for and on sexually explicit act or in a manner that may offend a reasonable adult on the computer resource or

(d) Facilitates abusing children online or

(e) records in any electronic form own abuse or that of others pertaining to sexually explicit act with children, *shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with a fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees*:

Provided that the provisions of section 67, section 67A and this section does not extend to any book, pamphlet, paper, writing, drawing, painting, representation or figure in electronic form

(i) The publication of which is proved to be justified as being for the public good on the ground that such book, pamphlet, paper writing, drawing, painting, representation or figure is in the interest of science, literature, art or learning or other objects of general concern; or

(ii) Which is kept or used for bonafide heritage or religious purposes

5.2.11. Section 67 C Preservation and Retention of information by intermediaries

(1) Intermediary shall preserve and retain such information as may be specified for such duration and in such manner and format as the Central Government may prescribe.

(2) Any intermediary who intentionally or knowingly contravenes the provisions of sub section (1) shall be punished with an imprisonment for a term which may extend to three years and shall also be liable to fine.

5.2.12. Section 69 Powers to issue directions for interception or monitoring or decryption of any information through any computer resource

(1) Where the central Government or a State Government or any of its officer specially authorized by the Central Government or the State Government, as the case may be, in this behalf may, if is satisfied that it is necessary or expedient to do in the interest of the sovereignty or integrity of India, defense of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above or for investigation of any offence, it may, subject to the provisions of sub-section (2), for reasons to be recorded in writing, by order, direct any agency of the appropriate Government to intercept, monitor or decrypt or cause to be intercepted or monitored or decrypted any information transmitted received or stored through any computer resource.

(2) The Procedure and safeguards subject to which such interception or monitoring or decryption may be carried out, shall be such as may be prescribed.

(3) The subscriber or intermediary or any person in charge of the computer resource shall, when called upon by any agency which has been directed under sub section (1), extend all facilities and technical assistance to –

(a) provide access to or secure access to the computer resource generating, transmitting, receiving or storing such information; or

(b) intercept or monitor or decrypt the information, as the case may be; or

(c) Provide information stored in computer resource.

(4) The subscriber or intermediary or any person who fails to assist the agency referred to in sub-section (3) shall be punished with an imprisonment for a term which may extend to seven years and shall also be liable to fine.

5.2.13. Section 69 A Power to issue directions for blocking for public access of any information through any computer resource

(1) Where the Central Government or any of its officer specially authorized by it in this behalf is satisfied that it is necessary or expedient so to do in the interest of sovereignty and integrity of India, defense of India, security of the State, friendly relations with foreign states or public order or for preventing incitement to the commission of any cognizable offence relating to above, it may subject to the provisions of sub-sections (2) for reasons to be recorded in writing, by order direct any agency of the Government or intermediary to block access by the public or cause to be blocked for access by public any information generated, transmitted, received, stored or hosted in any computer resource.

(2) The procedure and safeguards subject to which such blocking for access by the public may be carried out shall be such as may be prescribed.

(3) The intermediary who fails to comply with the direction issued under sub-section (1) shall be punished with an imprisonment for a term which may extend to seven years and also be liable to fine.

5.2.14. Section 69B Power to authorize to monitor and collect traffic data or information through any computer resource for Cyber Security

(1) The Central Government may, to enhance Cyber Security and for identification, analysis and prevention of any intrusion or spread of computer contaminant in the country, by notification in the official Gazette, authorize any agency of the Government to monitor and collect traffic data or information generated, transmitted, received or stored in any computer resource.

(2) The Intermediary or any person in-charge of the Computer resource shall when called upon by the agency which has been authorized under sub-section (1), provide technical assistance and extend all facilities to such agency to enable online access or to secure and provide online access to the computer resource generating, transmitting, receiving or storing such traffic data or information.

(3) The procedure and safeguards for monitoring and collecting traffic data or information, shall be such as may be prescribed.

(4) Any intermediary who intentionally or knowingly contravenes the provisions of subsection (2) shall be punished with an imprisonment for a term which may extend to three years and shall also be liable to fine.

5.2.15. Section 72 Breach of confidentiality and privacy

Save as otherwise provided in this Act or any other law for the time being in force, any person who, in pursuant of any of the powers conferred under this Act, rules or regulations made there under, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record, book, register, correspondence, information, document or other material to any other person shall be *punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.*

5.2.16. Section 72A Punishment for Disclosure of information in breach of lawful contract

Save as otherwise provided in this Act or any other law for the time being in force, any person including an intermediary who, while providing services under the terms of lawful contract, has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract, such material to any other person shall be *punished with imprisonment for a term which may extend to three years, or with a fine which may extend to five lakh rupees, or with both. Section 73 provides punishment for publishing a Digital Signature Certificate false in material particulars or otherwise making it available to any other person with imprisonment for a term which may extend to two years or with fine which may extend to Rs.1 lakh or with both.*

5.2.17. Section 76 Confiscation

Any computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto, in respect of which any provision of this Act, rules, orders or regulations made there under has been or is being contravened, shall be liable to confiscation

5.2.18. Section 77 B Offences with three years' imprisonment to be cognizable

Notwithstanding anything contained in Criminal Procedures Code, 1973, the offence punishable with imprisonment of three years and above shall be cognizable and the offence punishable with imprisonment of three years shall be bailable.

5.2.19. Section 78 Power to investigate offences

Notwithstanding anything contained in the Code of Criminal Procedure, 1973, a police officer not below the rank of Inspector shall investigate any offence under this Act.

5.2.20. Section 80 Power of Police Officer and Other Officers to Enter, Search, etc.

(1) Notwithstanding anything contained in the Code of Criminal Procedure, 1973, any police officer, not below the rank of an Inspector or any other officer of the Central Government or a State Government authorized by the Central Government in this behalf may enter any public place and search and arrest without warrant any person found therein who is reasonably suspected of having committed or of committing or of being about to commit any offence under this Act

5.2.21. Section 84 B

Punishment for abetment of offences (Inserted Vide ITA-2008): Whoever abets any offence shall, if the act abetted is committed in consequence of the abetment, and no express provision is made by this Act for the punishment of such abetment, be punished with the punishment provided for the offence under this Act.

5.2.22. Section 84 C Punishment for attempt to commit offences

Whoever attempts to commit an offence punishable by this Act or causes such an offence to be committed, and in such an attempt does any act towards the commission of the offence, shall, where no express provision is made for the punishment of such attempt, be punished with imprisonment of any description provided for the offence, for a term which may extend to one-half of the longest term of imprisonment provided for that offence, or with such fine as is provided for the offence or with both.

5.3. Other important provisions under Cr.P.C. for performing search & seizure

5.3.1. Section 165 Cr.P.C. Search by a police officer

(1) Whenever an officer in charge of police station or a police officer making an investigation has reasonable grounds for believing that anything necessary for the purposes of an investigation into any offence which he is authorised to investigate may be found in any place within the limits of the police station of which he is in charge, or to which he is attached, and that such thing cannot in his opinion be otherwise obtained without undue delay, such officer may, after recording in writing the grounds of his belief and specifying in such writing, so far as possible the thing for which search is to be made, search, or cause search to be made, for such thing in any place within the limits of such station.

(2) A police officer proceeding under sub-section (1), shall, if practicable, conduct the search in person.

(3) If he is unable to conduct the search in person, and there is no other person competent to make the search present at the time, he may, after recording in writing his reasons for so doing, require any officer subordinate to him to make the search, and he shall deliver to such subordinate officer an order in writing, specifying the place to be searched, and so far as possible, the thing for which search is to be made; and such subordinate officer may thereupon search for such thing in such place.

(4) The provisions of this Code as to search- warrants and the general provisions as to searches contained in section 100 shall, so far as may be, apply to a search made under this section.

(5) Copies of any record made under sub- section (1) or sub- section (3) shall forthwith be sent to the nearest Magistrate empowered to take cognizance of the offence, and the owner or occupier of the place searched shall, on application, be furnished, free of cost, with a copy of the same by the Magistrate.

5.3.2. Section 100 Persons in charge of closed place to allow search

(1) Whenever any place liable to search or inspection under this Chapter is closed, any person residing in, or being in charge of, such place, shall, on demand of the officer or other person executing the warrant, and on production of the warrant, allow him free ingress thereto, and afford all reasonable facilities for a search therein.
(2) If ingress into such place cannot be so obtained, the officer or other person executing the warrant may proceed in the manner provided by sub- section (2) of section 47.

(3) Where any person in or about such place is reasonably suspected of concealing about his person any article for which search should be made, such person may be searched and if such person is a woman, the search shall be made by another woman with strict regard to decency.

(4) Before making a search under this Chapter, the officer or other person about to make it shall call upon two or more independent and respectable inhabitants of the locality in which the place to be searched is situate or of any other locality if no such inhabitant of the said locality is available or is willing to be a witness to the search, to attend and witness the search and may issue an order in writing to them or any of them so to do.

(5) The search shall be made in their presence, and a list of all things seized in the course of such search and of the places in which they are respectively found shall be prepared by such officer or other person and signed by such witnesses; but no person witnessing a search under this section shall be required to attend the Court as a witness of the search unless specially summoned by it.

(6) The occupant of the place searched, or some person in his behalf, shall, in every instance, be permitted to attend during the search and a copy of the list prepared under this section, signed by the said witnesses, shall be delivered to such occupant or person.

(7) When any person is searched under sub- section (3), a list of all things taken possession of shall be prepared, and a copy thereof shall be delivered to such person.

(8) Any person who, without reasonable cause, refuses or neglects to attend and witness a search under this section, when called upon to do so by an order in writing delivered or tendered to him, shall be deemed to have committed an offence under section 187 of the Indian Penal Code (45 of 1860).

5.4. Admissibility of electronic records under Indian Evidence ACT

Section 65B of the Indian Evidence Act relates to admissibility of electronic records as evidence in the Court of law.

The computer holding the original evidence does not need to be produced in court.

5.4.1. 65A. Special provisions as to evidence relating to electronic record

The contents of electronic records may be proved in accordance with the provisions of section 65B.

5.4.2. 65B. Admissibility of electronic records

(1) Notwithstanding anything contained in this Act, any information contained in an electronic record which is printed on a paper, stored, recorded

Or

copied in optical or magnetic media produced by a computer (hereinafter referred to as the computer output) shall be deemed to be also a document, if the conditions mentioned in this section are satisfied in relation to the information and computer in question and shall be admissible in any proceedings, without further proof or production of the original, as evidence of any contents of the original or of any fact stated therein of which direct evidence would be admissible.

(2) The conditions referred to in sub-section (1) in respect of a computer output shall be the following, namely: -

(a) the computer output containing the information was produced by the computer during the period over which the computer was used regularly to store or process information for the purposes of any activities regularly carried on over that period by the person having lawful control over the use of the computer;

(b) during the said period, information of the kind contained in the electronic record or of the kind from which the information so contained is derived was regularly fed into the computer in the ordinary course of the said activities;

(c) throughout the material part of the said period, the computer was operating properly or, if not, then in respect of any period in which it was not operating properly or was out of operation during that part of the period, was not such as to affect the electronic record or the accuracy of its contents; and

(d) The information contained in the electronic record reproduces or is derived from such information fed into the computer in the ordinary course of the said activities.

(3) Where over any period, the function of storing or processing information for the purposes of any activities regularly carried on over that period as mentioned in clause (a) of sub-section

(2) was regularly performed by computers, whether

(a) By a combination of computers operating over that period; or

(b) By different computers operating in succession over that period; or

(c) By different combinations of computers operating in succession over that period; or

(d) in any other manner involving the successive operation over that period, in whatever order, of one or more computers and one or more combinations of computers, all the computers used for that purpose during that period shall be treated for the purposes of this section as constituting a single computer; and references in this section to a computer shall be construed accordingly.

(4) In any proceedings where it is desired to give a statement in evidence by virtue of this section, a certificate doing any of the following things, that is to say, -

(a) Identifying the electronic record containing the statement and describing the manner in which it was produced;

(b) giving such particulars of any device involved in the production of that electronic record as may be appropriate for the purpose of showing that the electronic record was produced by a computer;

(c) dealing with any of the matters to which the conditions mentioned in sub-section (2) relate, and purporting to be signed by a person occupying a responsible official position in relation to the operation of the relevant device or the management of the relevant activities (whichever is appropriate) shall be evidence of any matter stated in the certificate; and for the purposes of this sub-section it shall be sufficient for a matter to be stated to the best of the knowledge and belief of the person stating it.

(5) For the purposes of this section, -

(a) Information shall be taken to be supplied to a computer if it is supplied thereto in any appropriate form and whether it is so supplied directly or (with or without human intervention) by means of any appropriate equipment;

(b) whether in the course of activities carried on by any official, information is supplied with a view to its being stored or processed for the purposes of those activities by a computer operated otherwise than in the course of those activities, that information, if duly supplied to that computer, shall be taken to be supplied to it in the course of those activities;

(c) A computer output shall be taken to have been produced by a computer whether it was produced by it directly or (with or without human intervention) by means of any appropriate equipment.

Refer template of 65B certificate in Annexure 1 and a sample certificate in Annexure 2

5.5. Mapping of the offences against the relevant provisions of ITAA 2008

Sl. No.	Nature of complaint	Applicable section and punishment under ITAA 2008	Applicable section under other laws
1	Hacking of Email	Section 66 of ITAA 2008 - 3 years imprisonment or fine up to Rupees five lakh or both Section 66C of ITAA 2008 - 3 years imprisonment and fine up to Rupees one lakh	
2	Skimming of Credit Card/Debit Card	Section 66C of ITAA 2008- 3 years imprisonment and fine up to Rupees one lakh Section 66D ITAA 2008 - 3 years imprisonment and fine up to Rupees one lakh	Section 419 IPC - 3 years imprisonment or fine Section 420 IPC - 7 years imprisonment and fine
3	Creating impersonating websites for cheating. e.g. Job frauds	**Section 66C of ITAA 2008** 3 years imprisonment and fine up to Rupees one lakh Section 66D ITAA 2008 3 years imprisonment and fine up to Rupees one lakh	**Section 419 IPC** 3 years imprisonment or fine Section 420 IPC 7 years imprisonment and fine
4	Receiving stolen data	**Section 66 B of ITAA 2008** 3 years imprisonment or Rupees one lakh fine or both	**Section 411 IPC** 3 years imprisonment or fine or both
5	Source code theft or modification of source code or data or information without authorization	**Section 66 of ITAA 2008** 3 years imprisonment or fine up to rupees five lakh or both	
6	Identity Theft (Election card, Aadhaar, DL etc.,)	**Section 66C of ITAA 2008** 3 years imprisonment and fine up to Rupees one lakh	
7	A Phishing e-mail is sent in the name of bank asking card number, expiry date, CVV number	**Section 66D of ITAA 2008** 3 years imprisonment and fine up to Rupees one lakh	**Section 419 IPC** 3 years imprisonment or fine or both
8	Capturing, publishing, or transmitting the image of the private area without any person’s consent or knowledge	**Section 66E of ITAA 2008** Three years imprisonment or fine not exceeding Rupees two lakh or both	**Section 292 IPC** Two years imprisonment and fine Rupees 2000 and 5 years and rupees 5000 for second and subsequent conviction

Sl. No.	Nature of complaint	Applicable section and punishment under ITAA 2008	Applicable section under other laws
9	Sending phishing mail to compromise government network with virus, APT's, worms etc.,	**Section 66 of ITAA 2008** 3 years imprisonment or fine up to Rupees five lakh or both **Section 66F of ITAA 2008** Life imprisonment	
10	Perform DoS or DDoS attack on airlines, railways disrupting the essential servicers of the community	**Section 66 of ITAA 2008** 3 years imprisonment or fine up to Rupees five lakh or both **Section 66F of ITAA 2008** Life imprisonment	
11	Publishing or transmitting obscene material in electronic form	**Section 67 of ITAA 2008** first conviction - Three years and 5 lakh Second or subsequent conviction - 5 years and up to 10 lakh	**Section 292 IPC** Two years imprisonment and fine Rupees 2000 and five years and rupees 5000 for second and subsequent conviction
12	Publishing or transmitting of material containing sexually explicit act, etc., in electronic form	**Section 67A of ITAA 2008** first conviction - Five years and up to 10 lakh Second or subsequent conviction - 7 years and up to 10 lakh	Section 292 IPC - Two years imprisonment and fine Rupees 2000 and five years and rupees 5000 for second and subsequent conviction
13	Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc., in electronic form	**Section 67B of ITAA 2008** first conviction - Five years and up to 10 lakh Second or subsequent conviction - 7 years and up to 10 lakh	Section 292 IP - Two years imprisonment and fine Rupees 2000 and five years and rupees 5000 for second and subsequent conviction
14	Stealing data from armed forces, state/central government computers that have data or information related to national security.	**Section 66 of ITAA 2008** 3 years imprisonment or fine up to Rupees five lakh or both, **Section 66F of ITAA 2008** Life imprisonment	

Sl. No.	Nature of complaint	Applicable section and punishment under ITAA 2008	Applicable section under other laws
15	Not allowing the authorities to decrypt all communication that passes through your computer or network.	**Section 69 of ITAA 2008** Imprisonment up to 7 years and fine	
16	Intermediaries/ service providers (ISP, e-mail, Social media) not providing access to information stored on their computer to the relevant authorities	**Section 69 of ITAA 2008** Imprisonment up to 7 years and fine	
17	Posting defamatory messages on social media		**Section 500 IPC** 2 years or fine or both
18	E-mail Spoofing of a person and cheating	**Section 66C of ITAA 2008** 3 years imprisonment and fine up to Rupees one lakh	**Section 465 IPC** 2 years or fine or both **Section 468 IPC** 7 years imprisonment and fine

Annexures

Annexure-1

(____________Police Station
Crime No.   u/s________)
OR
(Certifying Organisation Letter Head)

CERTIFICATE UNDER SECTION 65(B) OF THE INDIAN EVIDENCE ACT, 1872

This is to certify that:

1. Printouts of all the documents/Data in CD/DVD/Pen drive were produced by the computer during the period over which the computer was used regularly to store and process information for the purposes of this activity.
2. That these outputs were produced by the computer of ______ (HP/DELL/ACER/etc.) company, which has been allotted to me by ________________ (organization/department) for official/business use.
3. This computer system is installed in _________ (place where the system is installed).
4. This computer system is used regularly to store or process information for the purpose of __________________ (business/official use).
5. Being a __________________________ (computer users designation/profile) I have got the lawful control over the use of this computer system.
6. During the said period, information contained in the electronic record derived was regularly fed into the computer in the ordinary course of the said activities.
7. Throughout the material part of the said period, the computer was operating properly.
8. The information contained in this electronic record reproduced or is derived from such information fed into the computer in the ordinary course of the said activities.

It has been stated to the best of my knowledge and belief.

(______________)

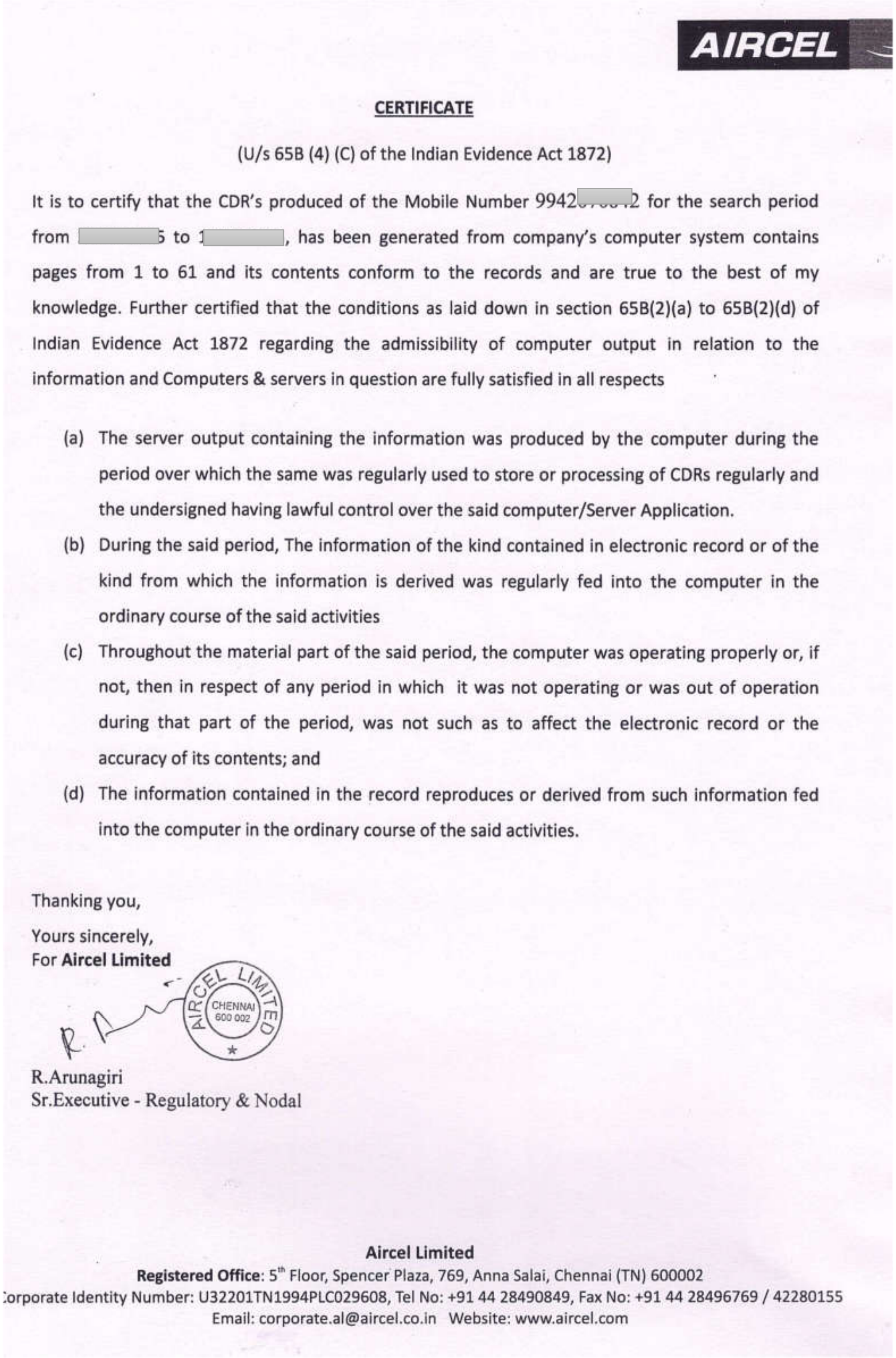
Date:

(certifying person sign
Name & designation)

Place:

Annexure-2

A sample copy of certificate u/s. 65B of IEA issued by MSP-Aircel for authenticating Call Data Records (CDR)



AIRCEL

CERTIFICATE

(U/s 65B (4) (C) of the Indian Evidence Act 1872)

It is to certify that the CDR's produced of the Mobile Number 9942[redacted]2 for the search period from [redacted]5 to 1[redacted], has been generated from company's computer system contains pages from 1 to 61 and its contents conform to the records and are true to the best of my knowledge. Further certified that the conditions as laid down in section 65B(2)(a) to 65B(2)(d) of Indian Evidence Act 1872 regarding the admissibility of computer output in relation to the information and Computers & servers in question are fully satisfied in all respects

(a) The server output containing the information was produced by the computer during the period over which the same was regularly used to store or processing of CDRs regularly and the undersigned having lawful control over the said computer/Server Application.

(b) During the said period, The information of the kind contained in electronic record or of the kind from which the information is derived was regularly fed into the computer in the ordinary course of the said activities

(c) Throughout the material part of the said period, the computer was operating properly or, if not, then in respect of any period in which it was not operating or was out of operation during that part of the period, was not such as to affect the electronic record or the accuracy of its contents; and

(d) The information contained in the record reproduces or derived from such information fed into the computer in the ordinary course of the said activities.

Thanking you,

Yours sincerely,
For **Aircel Limited**

AIRCEL LIMITED
CHENNAI
600 002

R.Arunagiri
Sr.Executive - Regulatory & Nodal

Aircel Limited
Registered Office: 5th Floor, Spencer Plaza, 769, Anna Salai, Chennai (TN) 600002
orporate Identity Number: U32201TN1994PLC029608, Tel No: +91 44 28490849, Fax No: +91 44 28496769 / 42280155
Email: corporate.al@aircel.co.in Website: www.aircel.com

Annexure-3

List of Nodal officers of Service Providers:

Nodal Service Providers List				
S no.	Name of the Service provider	Area Of Operation	Name of the Nodal Officer	Email ID/ Reporting Link
1	Facebook	All India	Vikram	https://www.facebook.com/records/login/
2	Instagram	All India		Same as above
3	Pinterest	All India		https://help.pinterest.com/en/law-enforcement
4	Twitter	All India		https://legalrequests.twitter.com/forms/landing_disclaimer lawenforcement@twitter.com
5	Google	All India	Gitanjali	gitanjli@google.com lis-apac@google.com
6	Microsoft	All India		indiacc@microsoft.com
7	Locanto	All India		support@locanto.in
8	GMAIL	All India	Legal Desk	lis-apac@google.com
9	Rediff	All India	LEA Support	customersupport@rediff.co.in legal@rediff.co.in
10	Sify	All India	LEA Support	lea.support@sifycorp.com
11	Skype	All India	Legal Desk	lerm@skype.net
12	Bharat Matrimony	All India		legal@consim.com
13	Ola	All India		cybercrimeescalations@olacabs.com, cccell@olacabs.com
14	Uber	All India		LERT@uber.com
15	Xvideos	All India		content@xvideos.com
16	mobikwik	All India		fraudalerts@mobikwik.com, risk@mobikwik.comrisk@mobikwik.com
17	oxigen	All India		fraud.control@myoxigen.com
18	Paytm One97Communication	All India		cybercell@paytm.com
19	flipkart.com	All India	Murthy	murthy.sn@flipkart.com, escalationdesk@flipkart.com
20	AMAZON	All India		police-inquiries@amazon.in, police-inquiries-India@amazon.in, cs-reply@amazon.in
21	Yahoo	All India	Mr. Robin	robinfe@yahoo-inc.com

Annexure-4

Recommended timetable Awareness course

Morning session

DAY	10:00 – 10:45	10:45 – 11:30	11:30 -11:45	11:45 – 12:30	12:30 - 13:15	13:15 14:15
1	Inauguration and Assessment Test	Introduction to Computer Hardware and other electronic devices and their terminology **(Chapter 2)**	Tea Break	Introduction to Internet and mobile technologies **(Chapter 1)**		Lunch Break
2	Introduction to social media like Facebook, Whatsapp etc. **(Chapter 4)**		Tea Break	Demonstration/ Hands on Practice on use of social media **(Chapter 4)**		Lunch Break
3	Recap of activities of Day 1 and Day 2	Relevant sections of IT Act and IPC **(Chapter 5)**	Tea Break	Basics of a Good cyber crime FIR / Report **(Chapter 3)**	Institutional set up for cybercrime investigation **(Chapter 3)**	Lunch Break

Afternoon session

DAY	14:15 15:00	15:00 15:45	15:45 16:00	16:00-16:45	16:45 17:30
1	An introduction to Cyber Crimes-general and specific to women & children **(Chapter 1)**		Tea Break	An introduction to Cyber Crimes-general and specific to women & children **(Chapter 1)**	
2	Introduction to online and cash less transactions like ATM, credit and debit cards, BHIM app, e-wallet, PayTM etc. **(Chapter 4)**		Tea Break	Demonstration/ Hands on Practice on online and cash less transactions like BHIM app, e-wallet, PayTM, ATM, credit and Debit cards etc. **(Chapter 4)**	
3	Counseling and advice to victims of cyber crime **(Chapter 3)**	Case studies and Advisories for public **(Chapter 3)**	Tea Break	Simulation Exercise **(Chapter 4)**	Assessment and Valedictory Session