DIGITAL & CYBER FORENSIC

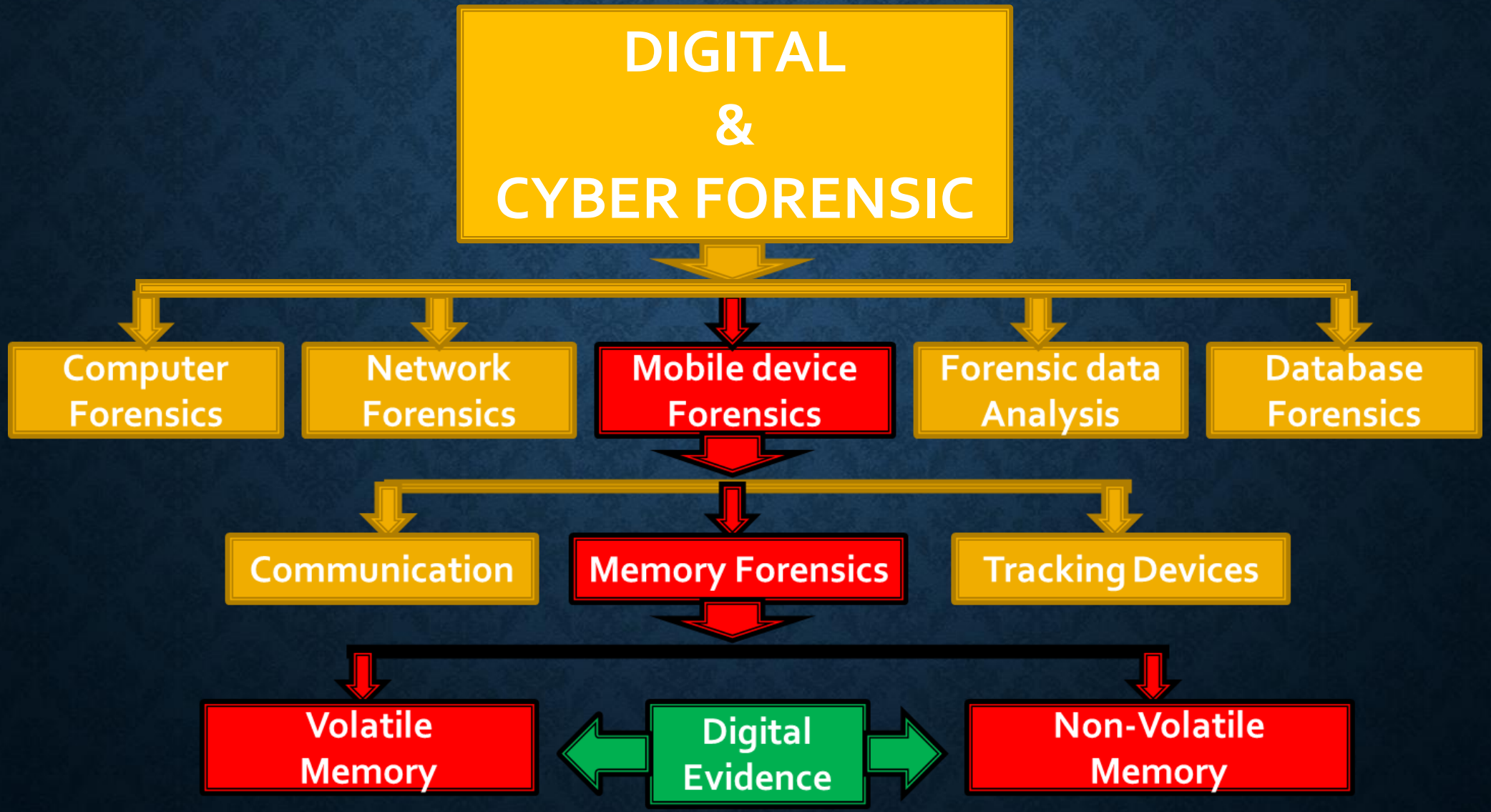
By

Parth Lakhalani

INTRODUCTION

- **Digital Forensic**
  - It is a branch of forensic science in which deal with investigation and recovery of digital evidence.
  - Digital forensics includes not only computers but also any digital device, such as digital networks, cell phones, flash drives and digital cameras.
- **Cyber Forensic or Computer Forensic**
  - Cyber Forensics is the scientific processes of identification, seizure, acquisition, authentication, analysis, documentation and preservation of digital evidence.

BRANCHES OF CYBER FORENSIC



INTRODUCTION

- **Digital Forensic**
  - It is a branch of forensic science in which deal with investigation and recovery of digital evidence.
  - Digital forensics includes not only computers but also any digital device, such as digital networks, cell phones, flash drives and digital cameras.
- **Cyber Forensic or Computer Forensic**
  - Cyber Forensics is the scientific processes of identification, seizure, acquisition, authentication, analysis, documentation and preservation of digital evidence.

INTRODUCTION

- **Network Forensic**
  - Network forensics is the capture, recording, and analysis of network events in order to discover the source of security attacks or other problem incidents.

- **Mobile (Device) Forensic**
  - Mobile device forensics is a branch of digital forensics relating to recovery of digital evidence or data from a mobile device under forensically sound conditions.

INTRODUCTION

- **Forensic data Analysis**
  - Forensic Data Analysis is a branch of digital forensics which examines structured data with the aim to discover and analyze patterns of fraudulent activities resulting from **financial crime**.
- **Database Forensic**
  - Database forensics is a branch of digital forensics relating to the forensic study of **databases and their metadata**.
  - Investigations use database contents, **log files and in-RAM data** to build a timeline or recover relevant information.

INTRODUCTION TO COMPUTER

By

Parth Lakhalani

INTRODUCTION

- **What is Computer?**

"Common Operating Machine

Purposely Used for

Technological and Educational Research"

- A computer is a machine that can be instructed to carry out sequences of arithmetic or logical operations automatically via computer programming.
- A computer is electronic Device (Programmable Device) that is used for processing of information and is capable of calculating and storing information

COMPONENT OF COMPUTER

Software Component

Software components of a computer system have no physical presence, they are stored in digital form within computer memory.

- System software
- Utilities
- Applications software.

Hardware Component

Hardware component includes the physical parts of a computer.

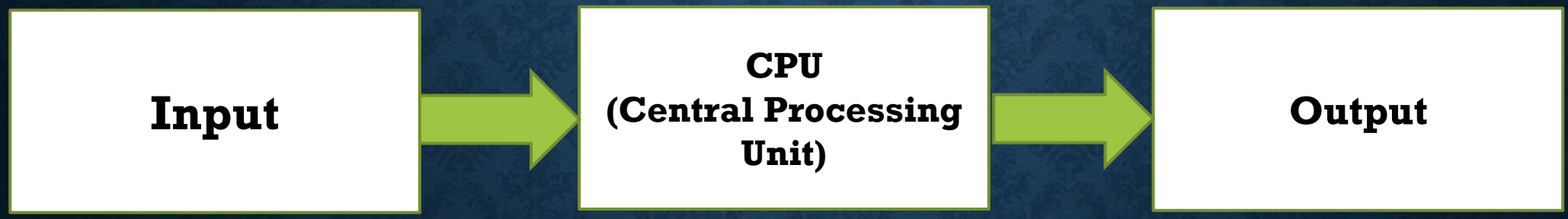
- Case, central processing unit (CPU),
- Input and output devices like monitor, mouse, keyboard,
- Computer data storage device(ROM),
- Graphics card,
- Sound card,
- Motherboard.

Power supply Component

Power supply Component converts mains AC to low-voltage regulated DC power for the internal components of a computer.

- Power supply Component also known as PSU (Power Supply Unit)

HOW COMPUTER WORKS



TRADITIONAL CRIME VS CYBER CRIME

By

Parth Lakhalani

Traditional crime	Cyber Crime
Traditional crimes are physically performed crimes.	Cyber crime are virtually performed crimes.
Eg. Robbery, Murder etc.	Eg. Phishing, Data stealing, Stalking etc.
Leaves some traces like Fingerprint or other physical evidence	Leaves no traces or less evidence
Difficult for criminal to alter their identity	Easily for criminal to alter their identity
Short period of time for investigation	Need longer period of time
Don't have protection of law and constitution	Protection of law and constitution
Rely on real evidence (easy to convince criminal)	Rely on virtual evidence (difficult to convince due to protection of law)
Possibility to finding real injuries make easy to investigate	No physical presence found, which makes more difficult to investigate

TRADITIONAL CYBER CRIME

By

Parth Lakhalani

INTRODUCTION TO TRADITIONAL CYBER CRIME

- The Computer crimes can be classified as: - Violent, Non-Violent computer crimes.
- The use of viruses, worms and Trojans to infect a system and to spread itself over the network is not new but the advancements achieved in these causes irreversible destruction to the infected system and the network.
- Computer crimes have risen so dramatically over the recent years that they have replaced the old-fashioned, organized crimes.

INTRODUCTION TO TRADITIONAL CYBER CRIME

- **What is Cyber crime?**
  - Cyber crimes refer to criminal activity where the computer or the network is the source, tool, target or place of the crime.
  - Cyber crimes in simple terms can be put as criminal activity involving an information technology infrastructure, including illegal access, illegal interception, data interference, and system interference, misuse of devices, forgery and electronic frauds.
  - Cybercrimes refers to criminal offences committed using the internet or another computer network as a component of the crime.

INTRODUCTION TO TRADITIONAL COMPUTER CRIME

- **Several different ways of Cybercrime**
  1. The computer or the network can be used to commit the crime.
  2. The computer or the network can be the target or the victim of the crime.
  3. The computer or the network can be used to store information related to certain crimes.

SEVERAL DIFFERENT TYPES OF COMPUTERCRIME

Violent or Potentially Violent crimes

- Have highest priorities
- Physical danger to both individuals and groups of people
- Against an individual or against any government body.
- Eg.
  1. Cyber Terrorism
  2. Assault by Threat
  3. Cyber Stalking
  4. Child Pornography & Child Abuse
  5. Harassment

  Etc.

Non-Violent Crimes

- Comparative less priorities then violent Crime
- Avoid Physical danger or any physical contact
- Against an individual or against any government body or Organizations.
- Eg.
  1. Cyber Frauds
  2. Cyber theft
  3. Drug Trafficking
  4. Phishing
  5. Cyber bullying

CLASSIFICATION OF CYBERCRIME

Against Individual

- This type of crime are very common in which attacker target to a specific person
- Eg.
  1. Email Spoofing
  2. Email Spamming
  3. Cyber Defamation
  4. Cyber Stalking

Against Property

- In this type criminal attack on property of any individual person or group's property.
- Eg.
  1. Credit Card Frauds
  2. Intellectual Property Crimes
  3. Internet Time Theft

Against Organization

- This type of crime is design to harm Organization's data or leak valuable data
- Eg.
  1. Unauthorized Access
  2. DoS attack
  3. Virus Attack
  4. Email Bombing
  5. Salami Attack
  6. Logic Bomb
  7. Trojan Horse
  8. Data Diddling

Against Society

- This type of crime are vary serious which harm to Society and it's property
- Eg.
  1. Forgery
  2. Cyber Terrorism
  3. Web Jacking

CRIMES AGAINST INDIVIDUALS

CLASSIFICATION OF CYBERCRIME

Against Individual

- This type of crime are very common in which attacker target to a specific person
- Eg.
  1. Email Spoofing
  2. Email Spamming
  3. Cyber Defamation
  4. Cyber Stalking

Against Property

- In this type criminal attack on property of any individual person or group's property.
- Eg.
  1. Credit Card Frauds
  2. Intellectual Property Crimes
  3. Internet Time Theft

Against Organization

- This type of crime is design to harm Organization's data or leak valuable data
- Eg.
  1. Unauthorized Access
  2. DoS attack
  3. Virus Attack
  4. Email Bombing
  5. Salami Attack
  6. Logic Bomb
  7. Trojan Horse
  8. Data Diddling

Against Society

- This type of crime are vary serious which harm to Society and it's property
- Eg.
  1. Forgery
  2. Cyber Terrorism
  3. Web Jacking

CRIMES AGAINST INDIVIDUALS

1. E-mail Spoofing

- A spoofing mail is the formation of email messages by impersonating correspondent identity. It shows its origin to be different from which actually it originates.
- **Example**
  - Rajesh Manyar, a Bachelor learner at Purdue University in Indiana, was under arrest for threatening to explode a nuclear device in the university campus. The suspected e- mail was sent from the account of another student to the vice president for student services. Though, the e-mail was tracked to be sent from the account of Rajesh Manyar.

CRIMES AGAINST INDIVIDUALS

2. E-mail Spamming

- Spam is a message also called as junk mail; send with a web link or business proposal.
- Clicking on this link or replying to commercial offer send to a phishing website or set up a malware in your workstation.
- The senders of this electronic mail are always unidentified. You need to be conscious to answering these kinds of spam mails because it tends towards some financial and data loss.

CRIMES AGAINST INDIVIDUALS

3. Cyber Defamation

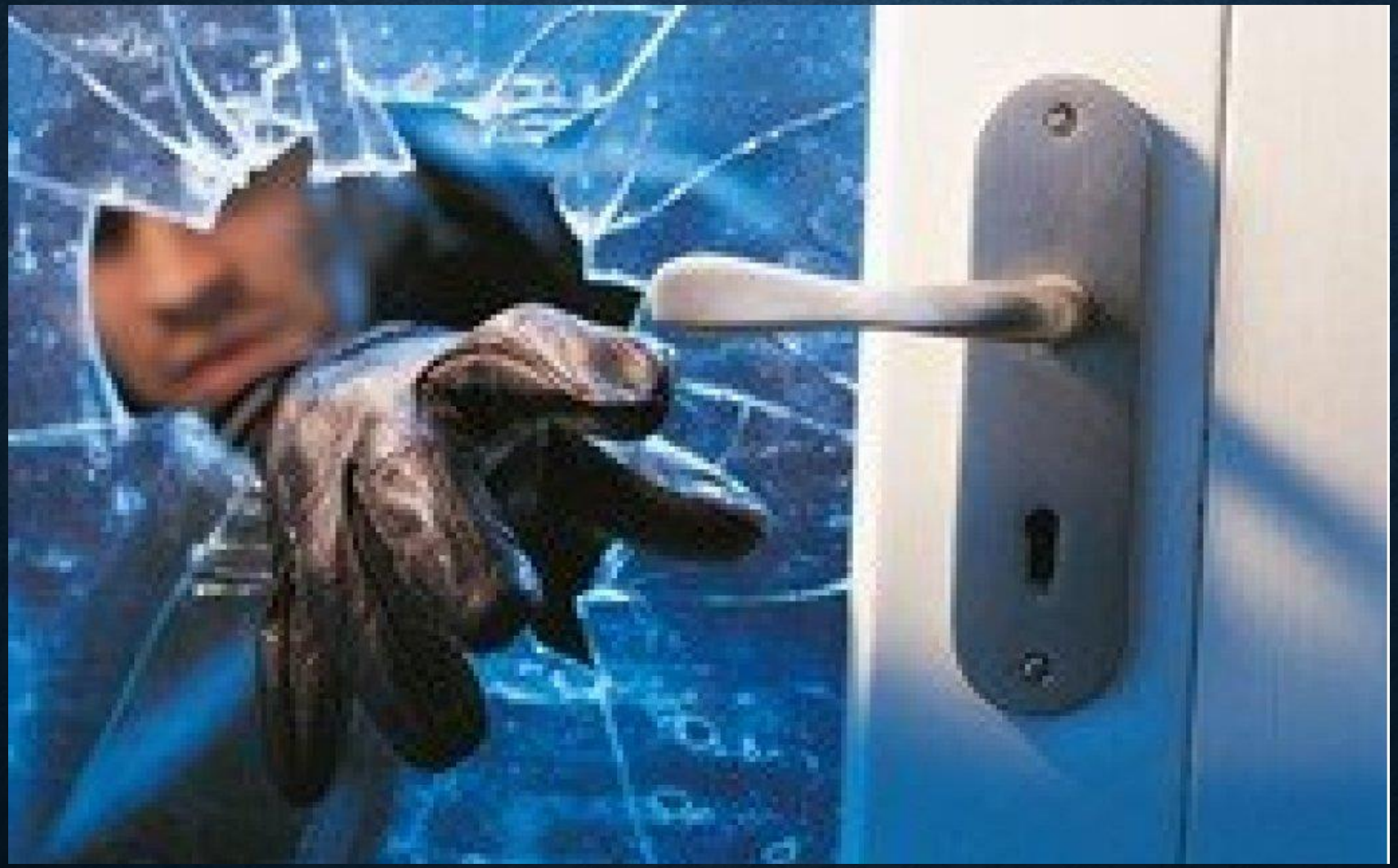
- It is an act of imputing any individual with intention to lower the person in the estimation of the right-thinking members of society generally or to cause him to be ignored or sidestepped or to rendering him to hate, disrespect or ridicule.
- Cyber defamation is not different from conventional defamation except the involvement of a virtual medium.
- E.g. the e-mail account of Rohit was hacked and several-mails were sent from his account to some of his colleague on the subject of his matter with a girl with intending to defame him.

CRIMES AGAINST INDIVIDUALS

4. Cyber Stalking

- The Oxford dictionary defines stalking as "pursuing stealthily".
- Cyber stalking involves following a person's movements across the Internet by posting messages (sometimes threatening) on the bulletin boards frequented by the victim, entering the chat-rooms visited by the victim, continually attacking the victim with emails, etc.

CRIMES AGAINST PROPERTY



CLASSIFICATION OF CYBERCRIME

Against Individual

- This type of crime are very common in which attacker target to a specific person
- Eg.
  1. Email Spoofing
  2. Email Spamming
  3. Cyber Defamation
  4. Cyber Stalking

Against Property

- In this type criminal attack on property of any individual person or group's property.
- Eg.
  1. Credit Card Frauds
  2. Intellectual Property Crimes
  3. Internet Time Theft

Against Organization

- This type of crime is design to harm Organization's data or leak valuable data
- Eg.
  1. Unauthorized Access
  2. DoS attack
  3. Virus Attack
  4. Email Bombing
  5. Salami Attack
  6. Logic Bomb
  7. Trojan Horse
  8. Data Diddling

Against Society

- This type of crime are vary serious which harm to Society and it's property
- Eg.
  1. Forgery
  2. Cyber Terrorism
  3. Web Jacking

CRIMES AGAINST PROPERTY

1. Credit Card Frauds

- Online fraud and cheating are most money-spinning trades that are rising nowadays in the cyber space.
- It may have diverse forms. Some of the cases of online fraud and cheating that are uncovered are those refer to credit card offences, contractual crimes, offering employment, etc.

CRIMES AGAINST PROPERTY

1. Credit Card Frauds

- Court of Metropolitan Magistrate Delhi found guilty a 24-year-old engineer employed in a call centre, of unfairly getting the details of Campa's credit card and bought a television and a cordless phone from Sony website. City magistrate Gulshan Kumar sentenced Azim for cheating under IPC, but does not direct him to jail.
- As an alternative, Azim was requested to provide a personal bond of Rs 20,000, and was released after a year of trial.

CRIMES AGAINST PROPERTY

2. Intellectual Property Crimes

- Intellectual property involves a list of rights. Any illegal act due to which, the owner is deprived entirely or partly of his human rights is a crime. The very common form of IPR abuse may be known to be software piracy, copyright infringement, trademark and service mark violation, theft of computer source code, etc.
- The Hyderabad Court in a land mark judgement has convicted 3 persons and sentenced them to 6 months custody and fine of 50,000 each for unauthorized copying and sell of pirated software.

CRIMES AGAINST PROPERTY

3. Internet Time Theft

- Basically, Internet time theft comes under hacking. It is the use by an unofficial individual, of the Internet hours paid for by another individual.
- The individual who gets entrance to someone else's ISP user ID and password, either by hacking or by gaining access to it by unlawful means, uses it to access the Internet devoid of the other person's knowledge.
- You can recognize time theft if your Internet time has to be recharged often, regardless of infrequent usage.

CRIMES AGAINST ORGANIZATION

CLASSIFICATION OF CYBERCRIME

Against Individual

- This type of crime are very common in which attacker target to a specific person
- Eg.
  1. Email Spoofing
  2. Email Spamming
  3. Cyber Defamation
  4. Cyber Stalking

Against Property

- In this type criminal attack on property of any individual person or group's property.
- Eg.
  1. Credit Card Frauds
  2. Intellectual Property Crimes
  3. Internet Time Theft

Against Organization

- This type of crime is design to harm Organization's data or leak valuable data
- Eg.
  1. Unauthorized Access
  2. DoS attack
  3. Virus Attack
  4. Email Bombing
  5. Salami Attack
  6. Logic Bomb
  7. Trojan Horse
  8. Data Diddling

Against Society

- This type of crime are vary serious which harm to Society and it's property
- Eg.
  1. Forgery
  2. Cyber Terrorism
  3. Web Jacking

CRIMES AGAINST ORGANIZATION

1. Unauthorized Access

- This is generally denoted to as ‘Hacking’. The Indian law has, however, given a different connotation to the term hacking, so we will not use the term "unauthorized access“
- It also known as term "hacking" to prevent misperception as the term used in the IT Act 2000 of India is much wider than hacking.

CRIMES AGAINST ORGANIZATION

2. Denial of Service Attack

- In simple words, Denial-of-Service referred the act by which a user of any website or service denied to use the service or website. In this category of cyber-crime, offenders aim the web server of the websites and flow a large number of requests to that server.
- This causes the use of maximum bandwidth of the website, and it goes slow down or not available for some times.

CRIMES AGAINST ORGANIZATION

3. Virus Attack

- A computer virus is a type of malware that, when executed, replicates by implanting the replicas of itself (probably altered) into other computer programs, data files or the boot sector of the hard drive;
- When this reproduction proceeds, the affected zones are then said to be "infected". Viruses frequently do certain type of dangerous activity on infected hosts, such as stealing hard disk space or CPU time, retrieving private information, corrupting data, displaying radical or funny mails on the user's display, spamming their links or logging their keystrokes.

CRIMES AGAINST ORGANIZATION

4. Email Bombing

- In email bombing, a user sending vast numbers of email to target address and due to this that email address or mail server crashed.
- It feels like Denial-of-service impression.
- It says that spamming is a variant of Email bombing.

CRIMES AGAINST ORGANIZATION

5. Salami Attack

- A salami attack is when minor attacks make up a major attack which becomes untraceable because of its nature. It is also called as Salami Slicing.
- Though salami slicing is frequently used to transport unlawful activities, it is only a plan for gaining an benefit over time by collecting it in small increments, so it can be used in perfectly legal ways as well.
- The attacker uses an online database to seize the information of customers that is bank/credit card details deducting very little amounts from every account above a period of time.
- The customers remain unaware of the slicing and hence no complaint is launched thus keeping the hacker away from detection.

CRIMES AGAINST ORGANIZATION

6. Logic Bomb

- A logic bomb is a piece of code intentionally inserted into a software system that will initiate mischievous features under definite conditions.
- For example, a programmer may hide a part of code that starts initiating deleting files (such as a salary database trigger), should they ever be completed from the company.

CRIMES AGAINST ORGANIZATION

6. Logic Bomb

- Software that is inherently malicious, such as viruses and worms, often contain logic bombs that execute a certain payload at a pre-defined time or when some other condition is met.
- This technique can be used by a virus or worm to gain momentum and spread before being noticed.
- Some viruses attack their host systems on particular dates, such as Friday the 13th or April fool's Day. Trojans that trigger on certain dates are frequently known as "time bombs".

CRIMES AGAINST ORGANIZATION

7. Trojan Horse

- A Trojan horse, or Trojan, in computing is a non-self-duplicating kind of malware program comprising malicious code that, when implemented, carries out actions determined by the nature of the Trojan, usually causing damage or stealing of data, and likely system damage.
- The term is derived from the tale of the wooden horse used to trick defenders of Troy into taking concealed warriors into their city in ancient Greece, because computer Trojans often hire a form of social engineering, representing themselves as routine, valuable, or interesting in order to encourage victims to install them on their computers.

CRIMES AGAINST ORGANIZATION

8. Data Diddling

- Data Diddling is illegal modifying of data. When an individual enters some data to his system and output is different from input then he may victim of data diddling.
- It is done by a virus program that changes the entered data.

CRIMES AGAINST SOCIETY

CLASSIFICATION OF CYBERCRIME

Against Individual

- This type of crime are very common in which attacker target to a specific person
- Eg.
  1. Email Spoofing
  2. Email Spamming
  3. Cyber Defamation
  4. Cyber Stalking

Against Property

- In this type criminal attack on property of any individual person or group's property.
- Eg.
  1. Credit Card Frauds
  2. Intellectual Property Crimes
  3. Internet Time Theft

Against Organization

- This type of crime is design to harm Organization's data or leak valuable data
- Eg.
  1. Unauthorized Access
  2. DoS attack
  3. Virus Attack
  4. Email Bombing
  5. Salami Attack
  6. Logic Bomb
  7. Trojan Horse
  8. Data Diddling

Against Society

- This type of crime are vary serious which harm to Society and it's property
- Eg.
  1. Forgery
  2. Cyber Terrorism
  3. Web Jacking

CRIMES AGAINST SOCIETY

1. Forgery

- When a perpetrator alters documents saved in electronic form, the crime committed may be forgery.
- In this instance, computer systems are the target of criminal activity.
- Computers, though, can also be used as tools with which to commit forgery.

CRIMES AGAINST SOCIETY

1. Forgery

- A new generation of fake modification or forging arise when electronic color laser duplicators became accessible.
- These duplicators are capable of high-resolution repetition, alteration of documents, and even the formation of false documents without getting an original, and they form documents whose quality is not differentiated from that of authentic documents except by an expert.

CRIMES AGAINST SOCIETY

2. Cyber Terrorism

- A terrorist means a person who indulges in wanton killing of persons or in violence or in disruption of services or means of communications essential to the community or indamaging property with the view to –

(1) Putting the public or any section of the public in fear; or

(2) Affecting adversely the harmony between different religious, racial, language or regional groups or castes or communities; or

(3) Coercing or overawing the government established by law;

(4) Endangering the sovereignty and integrity of the nation

CRIMES AGAINST SOCIETY

2. Cyber Terrorism

- a cyber-terrorist is the person who uses the computer system as a means or ends to achieve the above objectives.
- Every act done in pursuance thereof is an act of cyber terrorism.
- A cyber-crime is usually a domestic subject, which may have worldwide significances; though cyber terrorism is an international concern, which has domestic as well as international consequences.
- The common form of these terrorist attacks on the Internet is by dispersed denial of service attacks, hate websites and hate mails, attacks on delicate computer networks, etc.

CRIMES AGAINST SOCIETY

3. Web Jacking

- The word ‘Web Jacking’ comes from Hijacking.
- In this type of cyber-crime, the cybercriminals hacks the control of a website. They may able to change the content of that website.
- They use that website as owner and the real owner of website has no more control on the website.

THANK YOU

By

Parth Lakhalani

Mail: mr.parth141@gmail.com