Introduction

Outline

- Nature and scope of computer crime,
- Understanding how cyber criminals and hackers work
- Different types of cyber-crimes,
- Introduction to digital signatures,
- Cryptography,
- Digital certificate and public key infrastructure,
- IT Act.,
- Impact of cyber-crime on e-governance and e-commerce.

Cyber Crime

- Cybercrime refers to
  - criminal activities carried out
  - using computers and the internet,
  - including hacking, data theft, malware attacks, and financial fraud.

- With businesses, governments, and individuals relying heavily on digital platforms,
  - cyber threats have escalated,
  - leading to billions in financial losses worldwide.

Cyber Crime

- From phishing scams to Ransomware attacks,
  - cybercriminals exploit vulnerabilities
  - to steal sensitive information and disrupt systems.

- These crimes include:
- **Identity Theft**
- Stealing personal information to commit fraud.

- **Financial Fraud**
- Online scams, fake transactions, and credit card fraud.

Cyber Crime

- **Cyberbullying**
- Harassment or threats through digital platforms

- **Phishing Attacks**
- Deceptive emails or websites tricking users into revealing sensitive data

- **Hacking**
- Unauthorized access to systems and data breaches.

- **Malware Attacks**
- Spreading viruses, ransomware, and trojans to damage or steal data.

Cyber Crime

- Cybercriminals
- target individuals, businesses, and even government systems,
- leading to significant financial losses, data breaches, and security threats.

- As the internet becomes an essential part of daily life, from online shopping to business operations and communication, cybercrime cases have surged globally.

Cyber Crime

- Criminals
  - exploit system vulnerabilities to steal personal data,
  - manipulate financial transactions, and
  - disrupt critical services

Types of Cyber Crime

- Cybercrime includes
  - a wide range of illegal activities that exploit computers, networks, and the internet.

- These crimes can be categorized into two main types:

1. Cyber Crimes Targeting Computer Networks or Devices
2. Crimes Using Computer Networks to Commit Other Criminal Activities

1. Cyber Crimes Targeting Computer Networks or Devices

- These crimes involve direct attacks on computers, servers, or digital infrastructure to steal data, cause disruption, or damage systems.

- It involves different threats like
  - viruses,
  - bugs, etc. and
  - denial-of-service attacks.

Malware Attacks

- This kind of cyber threat relates to malware viruses, worms, Trojans, etc.
- for interfering, damaging, or unauthorized access to computer systems.

- **example**
- ransomware encrypts files and then later demands ransom for decryption.

Denial-of-Service (DoS) Attacks:

- the attackers focus on a system and flood it with high traffic,
- hence making it inaccessible to the users.
- Another dangerous variant of DoS is DDoS,
- wherein many compromised systems target one, thus, much difficult to defend against.
- **example**
- A DDoS attack crashes an e-commerce website by overwhelming its server with traffic.

Phishing Attacks

- These are
- masqueraded e-mails or messages
- claiming to be from a formal web but only request that the user grant access to sensitive information like password points for an account or credit card numbers.

- Phishing can be described as an outstanding one of the most common cyber threats.

- **example,**
- A fake PayPal login page that steals your credentials.

Botnets (Zombie Networks)

- A number of hijacked computers can become a "botnet" of malware that can be used by an attacker for coordinated attacks or spamming.

- **example,**
- Hackers use botnets to send millions of spam emails in a single day.

Exploits and Vulnerabilities

- The typical area through which cyber-thieves exploit software weakness is the application or operating system vulnerability in order to access it illegally.
- For example, Exploiting an outdated banking app to steal user financial details.

2. Crimes Using Computer Networks to Commit Other Criminal Activities

- These types of crimes include cyberstalking, financial fraud, or identity thief.

Cyberstalking

- crime in the nature of threatening or frightening a person online and spreading fear and emotional distress.

- This can be termed as involving threats, constant monitoring, or receiving repeated unwanted messages.

- For example, Sending threatening messages to a person via email or social media.

Financial Fraud

- This is an example of a cybercrook manipulating the victim online to proceed with stealing money, such as
- fake investment opportunities,
- hacking a business email, and
- using someone else's credit card details.

- For example, A fake online store that steals credit card details without delivering products.

Identity Theft

- It is normally the identity of people whose information is stolen with the intention of only acting like them either to misuse their cash or money from their account or even to do malicious reasons.

- It always lowers the credit score of the victim and in the worst case scenario, misused the account/loan financially with incorrect transactions.

- For example, A hacker using stolen credentials to apply for credit cards and loans.

Online Harassment and Hate Crimes

- When people use the internet to discriminate against a particular person based on his or her racial background, gender, religion, or whatever, which can psychologically disturb the harassed person.

- For example, Cyberbullying campaigns that target individuals based on race, gender, or religion.

Intellectual Property Theft

- Intellectual property theft refers to the theft of copyrighted content or business secrets through the internet,

- thereby financially and competitively hurting individuals and companies.

- For example, A software company illegally using another firm's source code to create a competing product.

Examples of Cyber Crime

- Cybercrime includes a wide range of illegal activities that exploit the internet, computer systems, and networks for financial, political, or personal gain.

- Here are some of the most common cybercrime examples:

1. Cyber Terrorism:

- Cyber terrorism involves using the internet to
  - carry out violent threats,
  - disrupt essential services, or spread fear among people.

- Cyber terrorists target critical infrastructure, government systems, or financial institutions to cause panic or damage.

- Example:
- Hacking into power grids or communication networks to create widespread disruption

2. Cyber Extortion (Ransomware Attackes):

- Cyber extortion happens when hackers attack websites or computer systems and demand money to stop the attacks.

- They threaten to keep attacking unless they receive a large payment.

- Example:
- A ransomware attack on a hospital system, blocking access to patient records until a ransom is paid

3. Cyber Warfare:

- Cyber warfare is when countries use computers and networks as part of their battles.

- It includes both attacking and defending against cyber threats, like hacking and spying.

- Example:
- A government hacking another country's defense networks to steal classified information.

4. Internet Fraud:

- This type of fraud occurs when someone tricks others on internet to steal money or private information.

- It involves hiding or giving false information to deceive people and covers many different illegal actions.

- Example:
- A scam website pretending to sell products but stealing users' payment details instead

5. Cyber Stalking and Online Harassement

- Cyber stalking is a form of online harassment where someone sends threatening messages or emails to a victim they know.

- If the stalker feels it's not working, they may also start following the victim in real life to make their life more difficult.

- Example:
- An ex-partner repeatedly sending threatening messages and tracking a victim’s online activity

6. Financial Fraud:

- Cybercriminals steal personal and financial data to commit fraud, open fake bank accounts, or make unauthorized transactions.

- Phishing attacks are one of the most common methods used to trick victims into providing sensitive information.

- Example:
- A phishing email pretending to be from a bank, asking users to enter their login details on a fake website.

7. Cyber Espionage:

- Cyber espionage refers to hacking into government agencies, businesses, or corporations to steal confidential data or trade secrets.

- It is often used by competitor businesses or state-sponsored hackers.

- Example:
- A company stealing another firm's product designs through hacking.

Challenges of Cyber Crime

- **People are unaware of their cyber rights:**
- The Cybercrime usually happen with illiterate people around the world who are unaware about their cyber rights implemented by the government of that particular country.

- **Anonymity:**
- Those who Commit cyber crime are anonymous for us so we cannot do anything to that person.

Challenges of Cyber Crime

- **Less numbers of case registered:**
- Every country in the world faces the challenge of cyber crime and the rate of cyber crime is increasing day by day because the people who even don't register a case of cyber crime and this is major challenge for us as well as for authorities as well.

- **Mostly committed by well educated people:**
- Committing a cyber crime is not a cup of tea for every individual.
- The person who commits cyber crime is a very technical person so he knows how to commit the crime and not get caught by the authorities.

Challenges of Cyber Crime

- **No harsh punishment:**
- In Cyber crime there is no harsh punishment in every cases.

- But there is harsh punishment in some cases like when somebody commits cyber terrorism in that case there is harsh punishment for that individual.

- But in other cases there is no harsh punishment so this factor also gives encouragement to that person who commits cyber crime.

Impact of Cyber Crimes

- **Financial Losses:**
- The fraud and theft can cause great losses not only for the given organizations but for individuals also.

- **Reputational Damage:**
- Some people may realize that reputation becomes an issue they may lose depending on the legal outcomes resulting from lawsuits.

Impact of Cyber Crimes

- **Operational Disruption:**
- As will be highlighted later, such an occurrence leads to a shutdown and consequently a loss of productivity.

- **Legal Consequences:**
- In the cases where clients have been involved in some legal cases or even regulatory fines, they may have to go through another phase of legal activities, clients have to spend considerable amount of money on protecting their data.

How to Protect Yourself Against Cybercrime?

- Use strong password
- Use trusted antivirus in devices
- Enable Two-Factor Authentication
- Keep your device software updated
- Use secure network
- Never open attachments in spam emails
- Software should be updated

How to Report a Cybercrime?

- Reporting cybercrime quickly is important to stop further damage and catch the criminals.

- Each country has its own way of handling cybercrime, but in most cases, you need to contact local police or a government agency that deals with online crimes.

How to Report a Cybercrime?

- **United States**

- **FBI's Internet Crime Complaint Center (IC3):**
- Victims can file complaints online at ic3.gov.
- This platform is designed for reporting cyber-enabled crimes and fraud.

How to Report a Cybercrime?

- **India**

- **National Cybercrime Reporting Portal:**
- Individuals can report cybercrimes through the official portal at cybercrime.gov.in.
- This service facilitates the online filing of complaints related to cyber offenses.

How to Report a Cybercrime?

- **European Union**

- **Europol's Reporting Page:**
- Europol provides links to national reporting websites for EU member countries.
- Visit Europol's website to find the appropriate platform for your country.