Module-II: Cybercrime and Cyber law
Classification of cyber crimes, Common cyber crimes- cyber crime targeting computers and mobiles, cyber crime against women and children, financial frauds, social engineering attacks, malware and ransomware attacks, zero day and zero click attacks, Cybercriminals modus-operandi, Reporting of cyber crimes, Remedial and mitigation measures, Legal perspective of cyber crime, IT Act 2000 and its amendments, Cyber crime and offences, Organizations dealing with Cybercrime and Cyber security in India, Case studies.

What are cyber crimes

- Cyber crimes are crimes that involve criminal activities done through cyberspace by devices connected to the internet.
- At times, cyber crimes are also called 'computer crimes'.
- The major objective of committing such crimes is to gather confidential data from people and use it for monetary, political, or personal motives.

Classification of cyber crimes

Classifying cybercrimes-broad and narrow

	Cybercrime in Narrow Sense	Cybercrime in Broad Sense	
Role of computer	**Computer as an object** The computer / information stored on the computer is the subject/target of the crime	**Computer as a tool** The computer/or information stored on the computer constitutes an important tool for committing the crime	**Computer as the environment or context** The computer / information stored on the computer play a non-substantial role in the act of crime, but does contain evidence of the crime
Examples	Hacking, sabotage, virtual child pornography	Computer fraud, forgery distribution of child pornography	Murder using computer techniques, bank robbery and drugs trade

cyber crimes can be classified under three heads, depending on the groups they are targeted at.

1. **Cyber crime against Individual**
   - Email spoofing: A spoofed email is one in which the e-mail header is forged so that the mail appears to originate from one source but actually has been sent from another source.
   - Spamming: Spamming means sending multiple copies of unsolicited mails or mass e-mails such as chain letters.
   - Cyber Defamation: This occurs when defamation takes place with the help of computers and/or the Internet. E.g. someone publishes defamatory matter about someone on a website or sends e-mails containing defamatory information.
   - Harassment & Cyber stalking: Cyber Stalking Means following an individual's activity over internet. It can be done with the help of many protocols available such as e- mail, chat rooms, user net groups.
2. **Cyber crime Against Property**
   - Credit Card Fraud: As the name suggests, this is a fraud that happens by the use of a credit card. This generally happens if someone gets to know the card number or the card gets stolen.
   - Intellectual Property crimes: These include Software piracy: Illegal copying of programs, distribution of copies of software. Copyright infringement: Using copyrighted material without proper permission. Trademarks violations: Using trademarks and associated rights without permission of the actual holder. Theft of computer source code: Stealing, destroying or misusing the source code of a computer.
   - Internet time theft: This happens by the usage of the Internet hours by an unauthorized person which is actually paid by another person.
3. **Cyber crime Against Organization**
   - Unauthorized Accessing of Computer: Accessing the computer/network without permission from the owner. It can be of 2 forms: a) Changing/deleting data: Unauthorized changing of data. b) Computer

voyeur: The criminal reads or copies confidential or proprietary information, but the data is neither deleted nor changed.

- Denial Of Service : When Internet server is flooded with continuous bogus requests so as to denying legitimate users to use the server or to crash the server.
- Computer contamination / Virus attack: A computer virus is a computer program that can infect other computer programs by modifying them in such a way as to include a (possibly evolved) copy of it. Viruses can be file infecting or affecting boot sector of the computer. Worms, unlike viruses do not need the host to attach themselves to.
- Email Bombing: Sending large numbers of mails to the individual or company or mail servers thereby ultimately resulting into crashing.
- Salami Attack: When negligible amounts are removed & accumulated in to something larger. These attacks are used for the commission of financial crimes.
- Logic Bomb: It is an event dependent program. As soon as the designated event occurs, it crashes the computer, release a virus or any other harmful possibilities.
- Trojan Horse: This is an unauthorized program which functions from inside what seems to be an authorized program, thereby concealing what it is actually doing.
- Data diddling: This kind of an attack involves altering raw data just before it is processed by a computer and then changing it back after the processing is completed.

4. Cyber crime Against Society

- Forgery : Currency notes, revenue stamps, mark sheets etc. can be forged using computers and high quality scanners and printers.
- Cyber Terrorism : Use of computer resources to intimidate or coerce people and carry out the activities of terrorism.
- Web Jacking : Hackers gain access and control over the website of another, even they change the content of website for fulfilling political objective or for money.

Cyber crime targeting computers and mobiles

- Cybercrime targeting computers and mobile devices is a growing concern in today's digital world.
- These crimes encompass a wide range of illegal activities conducted using technology, often with the goal of financial gain, data theft, or causing harm to individuals, organizations, or governments.
- Here are some common types of cybercrimes that target computers and mobiles:
    1. Malware Attacks: Malicious software (malware) is designed to infect computers and mobile devices. This includes viruses, worms, Trojans, ransomware, spyware, and adware. Malware can steal data, damage systems, or hold data hostage for a ransom.
    2. Phishing: Phishing attacks involve tricking individuals into revealing sensitive information like passwords, credit card numbers, or personal details by posing as a legitimate entity through email, text messages, or fake websites.
    3. Identity Theft: Cybercriminals can steal personal information, such as Social Security numbers and financial data, to commit fraud, open accounts in victims' names, or access their financial resources.
    4. Online Scams: Various online scams target individuals, such as advance-fee fraud, lottery scams, and romance scams. These scams deceive people into sending money or personal information to fraudsters.
    5. DDoS Attacks: Distributed Denial of Service (DDoS) attacks overwhelm a target's computer or network with traffic, making it unavailable to users. These attacks are often used to disrupt services or extort money.
    6. Data Breaches: Cybercriminals infiltrate organizations to steal sensitive data like customer information, trade secrets, or financial records. These breaches can result in significant financial losses and reputational damage.
    7. Cyberbullying: Cyberbullying involves the use of technology to harass, threaten, or intimidate individuals. It can take place through social media, messaging apps, or email.
    8. Mobile Device Theft and Hacking: Criminals can steal mobile devices for resale or hack into them to access personal data, financial information, or install malware.

9. Cyber Extortion: Criminals may threaten to release sensitive or embarrassing information unless a victim pays a ransom. This can involve sextortion (threatening to expose explicit content) or other forms of extortion.
10. Insider Threats: Employees or individuals with insider access to computer systems and data may misuse their privileges to steal or manipulate information.
11. Cryptojacking: Cybercriminals use a victim's computer or mobile device to mine cryptocurrency without their consent, which can slow down the device and increase energy consumption.

- To protect against cybercrime targeting computers and mobiles, individuals and organizations should implement robust cybersecurity measures, regularly update software, use strong passwords, be cautious when clicking on links or downloading files, and stay informed about the latest cyber threats and best practices.

Cyber crime against women and children

- Cybercrimes against women and children are particularly concerning because they often involve harassment, exploitation, or abuse of vulnerable individuals. Here are some common types of cybercrimes targeted at women and children:
    1. Cyberbullying: Both women and children can be victims of cyberbullying, which includes online harassment, threats, and intimidation. Perpetrators may use social media, messaging apps, or other digital platforms to target their victims.
    2. Online Harassment: This includes sending unsolicited, offensive, or threatening messages, images, or videos to women or children. It can be a form of cyberbullying and may have severe emotional and psychological effects.
    3. Revenge Porn: Perpetrators may share explicit or intimate images or videos of women without their consent, often as an act of revenge. This is a violation of privacy and can cause significant harm to victims.
    4. Sexting Exploitation: In cases involving children, sexting can lead to exploitation when someone coerces or blackmails minors into sharing explicit images or videos. This can have legal and psychological consequences for the child involved.

5. Online Grooming: Predators may use online platforms to groom children for sexual exploitation. They build trust with the child and gradually manipulate them into sharing personal information or engaging in inappropriate activities.
6. Child Pornography: The distribution, possession, or creation of child pornography is illegal and exploits children. Criminals often use the internet to share such material.
7. Online Trafficking: Human traffickers may use the internet to lure and exploit women and children, including for purposes of forced labor or sexual exploitation. Online platforms can be used to recruit victims.
8. Cyberstalking: This involves persistent and unwanted online attention, often leading to fear or emotional distress. Women and children can be targeted by cyberstalkers who may threaten or harass them through digital means.
9. Financial Fraud: Women can also be victims of financial fraud, including online scams targeting personal finances or online dating scams where perpetrators exploit emotional connections for financial gain.
10. Privacy Violations: Privacy breaches can occur when personal information or photographs are shared without consent, affecting both women and children. This can lead to identity theft or other forms of cybercrime.

- To combat cybercrimes against women and children, various organizations and governments have implemented laws and initiatives aimed at raising awareness, providing support to victims, and prosecuting offenders.

Financial frauds

- Financial frauds can have devastating consequences for individuals and the economy as a whole. While digital payments have made life convenient and easy In India, they have also made us prone to all kinds of financial frauds.
- **Ponzi Schemes: A Mirage of False Promises**
  - Ponzi schemes lure investors with promises of unusually high returns in a short period. The fraudsters use funds from new investors to pay off earlier investors, creating a false illusion of profitability.

- One infamous example is the **Saradha chit fund scam**, where millions of investors lost their hard-earned money. The group, consisting of over 200 private companies, falsely portrayed its collective investment schemes as chit funds.
- With an estimated collection of ₹200 to 300 billion (US$4–6 billion), the scheme managed to attract deposits from more than 1.7 million individuals before its eventual downfall.

- **Identity fraud**
  - Identity fraud is common on Internet. Criminals have a few options when it comes to stealing your sensitive information.
  - They might target you with a phishing attack where they email, call, or text pretending to be from your bank. Or, they could target you with a cyber attack to get you to install malware on your devices that steals your logins and passwords.
  - How do you know you're being targeted?
    - Unfamiliar transactions on your credit card.
    - Strange charges on your bank statements.
    - New credit cards or loans in your name.
    - Missing or error-filled tax returns.
    - Calls from debt collectors about purchases you didn't make.
    - A drop in credit score.
    - Bounced checks.
- **Fraudulent charities**
  - Scammers use philanthropy as fraud, too. Charity fraud entails creating a fake charity and collecting "donations" that disappear along with the thief
  - How does charity fraud happen?
    - Scammers create fake charities — like military veteran charities — that sound like ones you know and trust. These scams are especially common during natural disasters or international news events.
  - What are the warning signs?
    - Claiming that you're a previous donor when you know you've never sent them money.
    - Only accepting donations through cash, cryptocurrency, gift cards, or wire transfers

- **Credit card fraud**

- There are several ways that criminals can steal your credit card information. They could steal your physical card, trick you into entering information on a phishing website or email, buy your details on the Dark Web, or use any number of other credit card scams.
- Hackers can also create a clone of your physical card using just your credit card numbers.
- What are the warning signs?
  - Suspicious transactions on your credit card or bank statement.
  - Small unfamiliar charges on your account. (Fraudsters use a scam called carding to validate your credit card before making large purchases.)
  - Fraud alerts from your bank, credit card issuer, or credit monitoring service.

- **Stock Market Manipulation**

- Stock market manipulation includes activities like price rigging, spreading false information, insider trading, and pump-and-dump schemes. Fraudsters manipulate stock prices, deceiving investors and causing significant financial losses.
- The Satyam Computer Services scandal is a prime example, where the company's promoters manipulated financial statements to inflate stock prices.

- **Bank Frauds**

  - Bank frauds encompass various fraudulent activities, including loan frauds, cheque frauds, forged documents, and unauthorized transactions. These frauds result in substantial financial losses for banks and individuals.
  - One notable case is the Nirav Modi-PNB scam, where fraudulent Letters of Undertaking were issued, causing a massive loss to Punjab National Bank.

- **How to protect yourself against financial frauds**

  1. Protect your personal information
  2. Monitor financial activities
  3. Be cautious online
  4. Use strong passwords and enable two-factor authentication
  5. Stay informed about scams
  6. Keep your devices secure
  7. Exercise caution with public Wi-Fi
  8. Verify before sharing information

Social Engineering Attacks

Social Engineering

- It is the "technique to influence" & "persuasion to deceive" people to obtain the information.
- It exploits the fact that people are the weak link in security.
- Social engineers build the trust with the victim/person to gain the unauthorized information/access
- Their goal is to fool someone into providing valuable information.
- Example: The attacker (social engineer) calling a user & pretending to be a tech support person & ask questions about the confidential files, passwords, etc.

Classification of Social Engineering

1. **Human based Social Engineering:**

- It refers to person to person interaction to get the unauthorized information.
- The following are its different types.
    i. Impersonating an employee or valid user: The attacker impersonates/poses as an employee of the same organization to take the advantage from the people who are helpful.
    ii. Posing as important user: The attacker pretends to be a CEO/Manager who intimidates lower level employee in order to gain access to the system.
    iii. Using a third person: The attacker pretends to have permission from an authorized source/person (who cannot be contacted for verification) to use a system.
    iv. Calling technical support: Attacker calls help desk or tech support personnel to obtain the information since they are trained to help users.
    v. Shoulder surfing: It involves gathering information (usernames, passwords, etc) by watching over a person's shoulder while he/she logs into the system.
    vi. Dumpster diving (Scavenging/Binning): It involves looking in the trash/dustbin for information written on pieces of paper, computer print outs, etc.

2. **Computer based Social Engineering**

- It refers to the attempts made to get the unauthorized information by using computer/software/internet.

- The following are its different types.
  i. Fake emails: It involves the attacker sending fake emails (pretending as a legitimate email) to a number of users in order to make the users to reveal their sensitive information such as usernames, passwords, credit card details, etc. It is also called as Phishing.
  ii. Email attachments: It involves sending malicious codes to victim's system in the form of an email attachment. The virus, worms, etc which will be present in the email attachment will be automatically executed if the victim opens the attachment.
  iii. Pop-up windows: They are used similar to email attachments but they encourage the victim to click on special offers or free stuffs so that the malicious code can be installed to the system.

Effects of Social Engineering:

- Loss/altering of medical & healthcare information, corporate financial data, electronic funds transfers, etc.
- Loss of customers
- Loss of funds
- Loss of trust
- Collapse of the organization

Counter measures (Security) against Social Engineering:

- Providing training/awareness to the potential victims at regular intervals about the attacks
- Creating awareness on how attackers gain the trust of the victims
- Strict policies about service desk staff, not to ask for personal/sensitive information
- Educate potential victims to recognize social engineering attempt

Malware and Ransomware attacks

Malware Attacks

- Malware attacks are any type of malicious software designed to cause harm or damage to a computer, server, client or computer network and/or infrastructure without end-user knowledge
- Cyber attackers create, use and sell malware for many different reasons, but it is most frequently used to steal personal, financial or business information.

Types of Malware

1. Adware: Display ads (sometimes malicious ads) to users as they work on their computers or browse the web.
2. Viruses: A virus infects a computer and performs a variety of payloads. It may corrupt files, destroy operating systems, delete or move files, or deliver a payload at a specific date.
3. Worms: A worm is a self-replicating virus, but instead of affecting local files, a worm spreads to other systems and exhausts resources.
4. Trojans: A Trojan is named after the Greek war strategy of using a Trojan horse to enter the city of Troy. The malware masquerades as a harmless program, but it runs in the background stealing data, allowing remote control of the system, or waiting for a command from an attacker to deliver a payload.
5. Bots: Infected computers can become a part of a botnet used to launch a distributed denial-of-service by sending extensive traffic to a specific host.
6. Keyloggers: Capture keystrokes as users type in URLs, credentials, and personal information and send it to an attacker.
7. RAT: "Remote access tools" enable attackers to access and control the targeted device remotely.
8. Downloaders: Download other malware to install locally. The type of malware depends on the attacker's motives.
9. POS: Compromise a point-of-sale (PoS) device to steal credit card numbers, debit card and PINs, transaction history, and contact information.

How do I know I've been infected with malware?

- The most common signs that your computer has been compromised by malware are:
- Slow computer performance
- Browser redirects, or when your web browser takes you to sites you did not intend to visit
- Infection warnings, frequently accompanied by solicitations to buy something to fix them
- Problems shutting down or starting up your computer
- Frequent pop-up ads

How can I protect myself from malware?

1. **Protect your devices**
   - Keep your operating system and applications updated. Cybercriminals look for vulnerabilities in old or outdated software, so make sure you install updates as soon as they become available.
   - Never click on a link in a popup. Simply close the message by clicking on "X" in the upper corner and navigate away from the site that generated it.
   - Limit the number of apps on your devices. Only install apps you think you need and will use regularly. And if you no longer use an app, uninstall it.
2. **Be careful online**
   - Avoid clicking on unknown links. Whether it comes via email, a social networking site or a text message, if a link seems unfamiliar, keep away from it.
   - Be selective about which sites you visit. Do your best to only use known and trusted sites,
   - Beware of emails requesting personal information. If an email appears to come from your bank and instructs you to click a link and reset your password or access your account, don't click it. Go directly to your online banking site and log in there.
   - Avoid risky websites, such as those offering free screensavers.
3. **Perform regular checks**
   - If you are concerned that your device may be infected, run a scan using the security software you have installed on your device.
   - Check your bank accounts and credit reports regularly.

Ransomware Attack

- A ransomware attack is a malware that encrypts personal information and documents while demanding a ransom amount to decrypt them.
- Once the files are encrypted or locked behind a password, a text file is available to the victim, explaining how to make the ransom payment and unlock the files for it.

How Does a Ransomware Attack Work?

- The spread of ransomware mostly starts with phishing attacks. A ransomware attack gains access to a victim's device through infected emails, messages, and malicious sites and encrypts the data in that device.

- The ransomware uses simple asymmetric encryption algorithms, blocks a user's files, and makes them difficult to decrypt without knowing the key.
- Another way to breach a system with ransomware is by using the Remote Desktop Protocol or RDP access. It can access remotely a computer using this protocol, allowing a hacker to install malicious software on the system with the owner, unaware of these developments.
- Ransomware adds instruction files describing the pay-for-decryption process, then uses those files to present a ransom note to the user.
- Ransomware usually terminates and destroys itself by leaving only the payment instruction files.

Types of Ransomware

1. **Locker ransomware**
   - It is a type of malware that blocks standard computer functions from being accessed until the payment to the hackers is not complete.
   - It shows a lock screen that doesn't allow the victim to use the computer for primary purposes.

2. Crypto ransomware

- This ransomware encrypts the local files and documents on the computers.
- Once the files are encrypted, finding the decryption key is impossible unless the ransomware variant is old and the keys are already available on the internet.

3. Scareware

- It is a fake software that claims to have detected a virus or other issue on your computer and directs you to pay to resolve the problem.
- Some scareware locks the computer, while others flood the screen with pop-up alerts without damaging files.

How to Prevent Ransomware Attacks?

- One must always have backups of their data. Cloud storage for backup is easy, but a physical backup in a hard drive is always recommended.
- Keeping the system updated with the latest security patches is always a good idea.
- Apart from system updates, one must always have reputed antivirus software installed.

- If a system is infected with ransomware already, there is a website, 'nomoreransom.org.' It has a collection of decryption tools for most well-known ransomware packages.

Zero day and Zero click attacks

Zero day

- Software often has security vulnerabilities that hackers can exploit to cause havoc.
- The term "zero-day" refers to the fact that the vendor or developer has only just learned of the flaw – which means they have “zero days” to fix it.
- A zero-day attack takes place when hackers exploit the flaw before developers have a chance to address it.
- Zero-day attackers can steal data, corrupt files, take control of devices, install malware or spyware, and more.
- Typical targets for a zero-day exploit include:
  1. Government departments.
  2. Large enterprises.
  3. Individuals with access to valuable business data, such as intellectual property.
  4. Hardware devices, firmware and Internet of Things (IoT).

Recent Examples of Zero Day Attacks

- In December 2021, Amazon Web Services, Microsoft, Cisco, Google Cloud, and IBM were among the major tech players affected by the Log4j vulnerability in an open-source logging library.
- In 2021, Google's Chrome suffered a series of zero-day threats, causing Chrome to issue updates. The vulnerability stemmed from a bug in the V8 JavaScript engine used in the web browser.
- Zoom was targeted in 2020. Hackers were able to remotely access users’ PCs if the video conferencing platform was running on an older version of Windows.
- Apple’s iOS fell victim in 2020 to two sets of zero-day bugs that saw attackers compromising iPhones remotely.

How to protect yourself against zero-day attacks

1. **Keep all software and operating systems up to date.** This is because the vendors include security patches to cover newly identified vulnerabilities in new releases. Keeping up to date ensures you are more secure.
2. **Use only essential applications.** The more software you have, the more potential vulnerabilities you have. You can reduce the risk to your network by using only the applications you need.
3. **Use a firewall.** A firewall plays an essential role in protecting your system against zero-day threats. You can ensure maximum protection by configuring it to allow only necessary transactions.

Zero click

- zero-click attacks require no action from the victim – meaning that even the most advanced users can fall prey to serious cyber hacks and spyware tools.
- also called interaction-less or fully remote attacks.
- spying software relies on convincing the targeted person to click on a compromised link or file to install itself on their phone, tablet, or computer.
- However, with a zero-click attack, the software can be installed on a device without the victim clicking on any link. As a result, zero-click malware or no-click malware is much more dangerous.
- The target of a zero-click attack can be anything from a smartphone to a desktop computer and even an IoT device

Examples of Zero-Click Attacks

1. **Apple zero-click, forced entry, 2021:** In 2021, a Bahraini human rights activist had their iPhone hacked by powerful spyware sold to nation-states.
2. **WhatsApp breach, 2019:**This infamous breach was triggered by a missed call, which exploited a flaw in the source code framework of WhatsApp.

How to protect yourself from zero-click exploits

- Keep your operating system, firmware, and apps on all your devices up to date as prompted.
- Only download apps from official stores.
- Delete any apps you no longer use.
- Use your device password protection.
- Use strong authentication to access accounts, especially critical networks.
- Use strong passwords – i.e., long and unique passwords.

Modus Operandi of Cyber Criminals

- In general, modus operandi is the method acquired by any criminal for the successful commission of a crime. At a minimum, every Modus Operandi will contain three basic elements namely:
    1. Ensure success of the crime
    2. Protect identity
    3. Facilitate effective escape

Common forms of modus operandi

1. **Sending Annoying Messages**
    - Annoying, Insulting, Misleading, Defaming messages are often sent using mobile phones in bulk. Hence the actual source could not be fixed.
    - Such messages are often a cause of misperception among people of different race, culture and tradition many a times often resulting in fights or riots.
    - Unaware and innocent people often fall in traps of cyber criminals for SMS of lottery, Emails of prize money, false promise of jobs, and false mail for admission in reputed colleges.
    - Multimedia messages often defaming the identity of a person are distributed among small groups using mobile phones.
    - Pornography, Obscene messages and cyber bullying are becoming very common and very popular, for e.g. Delhi MMS Scandal.
    - Obscene videos are often captured in remote places unknowingly of the victim for future exploitation.

2. **Making Offensive Calls**
   - Offenders can also harass others by making offensive calls to them and annoying them.
   - Many a time anonymous calls are used by the criminals as an effective tool in making extortion or threatening call. Females are often harassed by stalkers by this means of communication.
   - Landlines having no Caller Ids pose a problem for the quick analysis of an incoming call, which is an undue advantage to the cyber stalkers, cyber bullies, etc.
   - Calls can be made by spoofing the mobile number using various sites. Such calls are intended to hide the actual location of the caller and any fake or annoying calls are made. Such calls are often used for terrorist activity and for trafficking illegal goods or for any ransom or blackmailing purposes.
   - Cyber Criminals operating from overseas and indulged in forgery are hard to trace without the co-operation of international agencies.

Reporting of cyber crimes

- Reporting cybercrimes is essential to combat online threats and hold perpetrators accountable. Here are the steps you can take to report cybercrimes:

1. **Contact Your Local Law Enforcement:** If you believe you are a victim of a cybercrime, you should report it to your local police department or law enforcement agency. They can investigate the incident and take appropriate action.
2. **Report to a National Cybersecurity Agency:** In many countries, there are dedicated agencies responsible for handling cybercrimes. In the United States, for example, you can report cybercrimes to the Federal Bureau of Investigation (FBI) through their Internet Crime Complaint Center (IC3). Check if your country has a similar agency and report the incident to them.
3. **Report to the Appropriate Online Platforms:** If the cybercrime occurred on a specific online platform, such as a social media site, email service, or e-commerce website, report the incident to that platform. They may have mechanisms in place to address various online abuses and can take action against the responsible parties.
4. **Report to Anti-Fraud Organizations:** There are organizations like the Anti-Phishing Working Group (APWG) and the Anti-Malware Testing Standards Organization (AMTSO) that collect

information about cyber threats and work with law enforcement. Reporting incidents to these organizations can help in identifying trends and patterns.

5. **Report to Financial Institutions:** If the cybercrime involves financial fraud, contact your bank or financial institution immediately. They can help you secure your accounts and investigate any unauthorized transactions.
6. **Report to Internet Service Providers (ISPs):** If you have evidence of cybercrimes, such as hacking or distribution of illegal content, involving an IP address, contact the relevant Internet Service Provider (ISP). They may take action against the offender or provide assistance to law enforcement.
7. **Document the Incident:** Make sure to document all evidence related to the cybercrime, including emails, messages, screenshots, IP addresses, and any other relevant information. This documentation can be crucial for investigations.
8. **Use Online Reporting Portals:** Many countries and regions have online reporting portals where you can report cybercrimes. These portals may be managed by government agencies or law enforcement. Check if your region offers such a service.
9. **Consider Legal Advice:** In some cases, it may be necessary to seek legal advice or consult with a cybersecurity expert to understand the best course of action and to help with the investigation.
10. **Protect Yourself:** While reporting the cybercrime, take steps to secure your online presence, change passwords, update security settings, and install or update security software to prevent further incidents.

- Remember that reporting cybercrimes is essential for both your own protection and the collective effort to combat online threats. The information you provide can help authorities take action and prevent future cybercrimes.

Remedial and mitigation measures

Remedial Measures:

1. **Incident Response:** In the event of a cyber crime, organizations should have an incident response plan in place to quickly identify, contain, and mitigate the impact of the attack. This includes isolating affected systems, restoring backups, and applying patches or security updates.

2. **Forensic Investigation:** Engaging professional forensic investigators can help identify the source and extent of the cyber crime, gather evidence, and aid in legal proceedings.
3. **Data Recovery:** If data is compromised or encrypted due to a cyber attack, organizations should have backups in place to restore affected systems and minimize data loss.

Mitigation Measures:

1. **Strong Security Practices:** Implement robust security measures, such as firewalls, antivirus software, and intrusion detection and prevention systems, to protect against cyber threats.
2. **Regular Updates and Patching:** Keep software, operating systems, and firmware up to date with the latest security patches to mitigate vulnerabilities that cyber criminals may exploit.
3. **Employee Education:** Provide cybersecurity awareness and training programs to employees to educate them about common cyber threats, phishing techniques, and safe online practices.
4. **Multi-factor Authentication (MFA):** Implement MFA wherever possible to add an extra layer of security, making it harder for cyber criminals to gain unauthorized access to accounts or systems.
5. **Data Encryption:** Encrypt sensitive data, both in transit and at rest, to ensure that even if it is intercepted or stolen, it remains unreadable and unusable for unauthorized individuals.
6. **Regular Security Audits:** Conduct regular security audits and vulnerability assessments to identify and address any weaknesses or potential entry points for cyber criminals.

Legal perspective of cyber crime

- In today's techno-savvy environment, the world is becoming more and more digitally sophisticated and so are the crimes.
- All legal issues related to internet crime are dealt with through cyber laws.
- As the number of internet users is on the rise, the need for cyber laws and their application has also gathered great momentum.
- **Cyber law** is a framework created to give legal recognition to all risks arising out of the usage of computers and computer networks.
- Cyber law encompasses laws relating to:
    1. Cyber crimes
    2. Electronic and digital signatures

3. Intellectual property
4. Data protection and privacy

Legal perspective of cybercrime in India

- In India, cybercrime is primarily governed by the Information Technology Act, 2000 (IT Act). This law was established to address various cyber offenses and provide a legal framework for electronic transactions, digital signatures, and data protection.
- The purpose of the Indian IT Act(ITA) was to amend the Indian Penal Code(IPC).

Section Reference And Title	Chapter of the Act and Title	Crime	Punishment
Sec. 43 (Penalty for damage to computer system, etc.)	Chapter IX Penalties and Adjudication	Damage to computer system, etc.	Compensation for Rs. 1 Crore.
Sec. 66 (Hacking with computer system)	Chapter XI Offences	Hacking (With intent or knowledge).	Fine of Rs. 2 lakhs and imprisonment for 3 years.
Sec. 67 (Publishing of information which is obscene in electronics form).	Chapter XI Offences	Publication of obscene material in electronic form.	Fine of Rs. 1 lakh, of imprisonment for 5 years and double conviction on second offence.
Sec. 68 (Power of controller to give directions).	Chapter XI Offences	Not complying with directions of controller.	Fine up to Rs. 2 lakhs and imprisonment of 3 years.
Sec. 70(Protected system)	Chapter XI Offences	Attempting or securing access to computer of another person without his/her knowledge.	Imprisonment up to 10 years.
Sec.72(Penalty for breach of confidentiality and privacy)	Chapter XI Offences	Attempting or securing access to computer for breaking confidentiality of the information of computer.	Fine up to Rs. 1 lakh and imprisonment up to 2 years.
Sec.73(Penalty for publishing digital signature Certificates false in certain particulars)	Chapter XI Offences	Publishing false digital signatures, false in certain particulars.	Fine of Rs. 1 lakh or imprisonment of 2 years or both.
Sec.74(Publication for fraudulent purpose)	Chapter XI Offences	Publication of Digital Signatures for fraudulent purpose.	Imprisonment for the term 2 years and fine of Rs. 1 lakh.

The key provisions under the Indian ITA 2000

Amendments and Updates

- The IT Act has undergone amendments over the years to address emerging cyber threats and strengthen cybercrime provisions.
- For example, the Information Technology (Amendment) Act, 2008 introduced additional provisions to tackle cyber terrorism, data privacy, and intermediary liability.
- It is important to consult with legal professionals or refer to official sources for comprehensive and up-to-date information on the legal aspects of cybercrime in India.

Cyber crime and offences

- Cybercrime encompasses various illegal activities conducted through digital means, often targeting individuals, organizations, or systems. Here are some common cybercrimes and offenses:

1. **Hacking:** Unauthorized access to computer systems, networks, or devices to manipulate, steal data, or disrupt operations.
2. **Identity Theft:** Stealing personal information (such as Social Security numbers, credit card details) to impersonate someone else, commit fraud, or gain access to financial resources.
3. **Phishing and Spoofing:** Sending deceptive emails or creating fake websites to trick individuals into revealing sensitive information (passwords, financial data) or downloading malware.
4. **Cyberbullying:** Harassment, threats, or intimidation using digital platforms, often directed at individuals, which can have serious emotional and psychological effects.
5. **Online Fraud:** Illegitimate schemes to deceive individuals or entities for financial gain, including investment scams, online shopping fraud, and auction fraud.
6. **Distributed Denial of Service (DDoS) Attacks:** Overloading servers or networks with excessive traffic to disrupt access, making websites or services unavailable to users.
7. **Cyber Espionage:** Unauthorized access to confidential information or intellectual property of governments, organizations, or individuals, often carried out by other governments or corporate entities.
8. **Child Exploitation and Pornography:** Using digital means to produce, distribute, or possess child pornography or engage in illegal activities involving minors.
9. **Ransomware Attacks:** Malicious software that encrypts files or systems, demanding payment (usually in cryptocurrency) for decryption or to avoid data exposure.
10. **Cyberstalking:** Persistent harassment or monitoring of an individual online, causing fear or emotional distress.

Organizations dealing with Cybercrime and Cyber security in India,

- In India, several organizations are involved in dealing with cybercrime and cybersecurity at various levels, including law enforcement, regulatory bodies, and agencies focused on awareness and prevention.
- Some prominent ones include:
    1. **National Cyber Security Coordinator (NCSC):** The NCSC operates under the Prime Minister's Office and is responsible for coordinating all cybersecurity initiatives in the country.

2. **Computer Emergency Response Team-India (CERT-In):** CERT-In is the national nodal agency under the Ministry of Electronics and Information Technology that deals with cybersecurity incidents, response, and related issues.
3. **National Critical Information Infrastructure Protection Centre (NCIIPC):** NCIIPC is responsible for protecting critical information infrastructure in the country and formulating policies and guidelines for securing these assets.
4. **State Police Cyber Cells:** Many states have established specialized cyber cells within their police departments to investigate and handle cybercrimes at the state level.
5. **National Investigation Agency (NIA):** NIA deals with investigating and prosecuting offenses affecting the sovereignty, security, and integrity of India, including cybercrimes with national implications.
6. **Cyber Appellate Tribunal (CAT):** It hears appeals against any order passed by CERT-In or the Adjudicating Officer under the Information Technology Act, 2000.
7. **Banks and Financial Institutions:** Regulatory bodies like the Reserve Bank of India (RBI) and Securities and Exchange Board of India (SEBI) have guidelines and teams dedicated to cybersecurity in the financial sector.
8. **Private Cybersecurity Firms:** Several private cybersecurity companies operate in India, offering services ranging from consulting and risk assessment to incident response and security solutions.

- These organizations collaborate to address cyber threats, enforce cybersecurity laws and regulations, provide guidelines and advisories, conduct awareness programs, and investigate cybercrimes. They play a crucial role in safeguarding digital infrastructure and combating cyber threats in India.