Program : **B.Tech**

Subject Name: **Cyber Security**

Subject Code: **CS-503**

Semester: **5th**

Unit-3

Topics to be covered

UNIT 3

Cyber Crime and Criminal justice: Concept of Cyber Crime and the IT Act, 2000, Hacking, Teenage Web Vandals, Cyber Fraud and Cheating, Defamation, Harassment and E-mail Abuse, Other IT Act Offences, Monetary Penalties, jurisdiction and Cyber Crimes, Nature of Criminality, Strategies to tackle Cyber Crime and Trends.

Cyber Crime- Cyber Crime, or computer oriented crime, is crime that involves a computer and a network. The computer may have been used in the commission of a crime, or it may be the target. Cybercrime is a Offences that are committed against individuals or groups of i individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (networks including but not limit end to Chat rooms, emails, notice boards and groups) and mobile phones (Bluetooth/SMS/MMS).Cybercrime may threaten a person or a nation's security and financial health. Issues surrounding these types of crimes have become high - profile, particularly those surrounding hacking, copyright infringement, unwarranted mass-surveillance, Sextortion, child pornography, a n d child grooming. There arealso problems of privacy when confidential information is intercepted or disclosed, lawfully or otherwise.

IT Act, 2000-An Act to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as electronic commerce, which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, the Indian Evidence Act, 1872, the Banker's Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto. Cybercrimes are a new class of crimes which are increasing day by day due to extensive use of internet these days. To combat the crimes related to internet The Information Technology Act, 2000 was enacted with prime objective to create an enabling environment for commercial use of I.T. The IT Act specifies the acts which have been made punishable. The Indian Penal Code, 1860 has also been amended to take into its purview cybercrimes. The various offenses related to internet which have been made punishable under the IT Act and the IPC are enumerated below:

Cybercrimes under the IT Act

- Tampering with Computer source documents - Sec.65
- Hacking with Computer systems, Data alteration - Sec.66
- Publishing obscene information - Sec.67
- Un-authorized access to protected system Sec.70 Breach of Confidentiality and Privacy - Sec.72
- Publishing false digital signature certificates - Sec.73

Cyber Crimes under IPC and Special Laws

- Sending threatening messages by email - Sec 503 IPC
- Sending defamatory messages by email - Sec 499 IPC
- Forgery of electronic records - Sec 463 IPC
- Bogus websites, cyber frauds - Sec 420 IPC
- Email spoofing - Sec 463 IPC
- Web-Jacking - Sec. 383 IPC
- E-Mail Abuse - Sec.500 IPC

Cyber Crimes under the Special Acts

- Online sale of Drugs under Narcotic Drugs and Psychotropic Substances Act

- Online sale of Arms Act

The newly amendment Act came with following highlights;

- It focuses on privacy issues.
- It focuses on Information Security.
- It came with surveillance on Cyber Cases.
- The Concept of Digital Signature was elaborated.
- It clarified reasonable security practices for corporate.
- Role of Intermediaries were focuses.
- It came with the Indian Computer Emergency Response Team.
- New faces of Cyber Crime were added.
- Powers were given to Inspector to investigate cyber-crimes as against only to DSP.
- Severe Punishments and fine were added.

Hacking-Hacking is unauthorized intrusion into a computer or a network. The person engaged in hacking activities is generally referred to as a hacker. This hacker may alter system or security features to accomplish a goal that differs from the original purpose of the system.
Hackers are classified according to the intent of their actions. The following list classifies hackers according to their intent.

Ethical Hacker (White hat): A hacker who gains access to systems with a view to fix the identified weaknesses. They may also perform penetration testing and vulnerability assessments.
Ethical hackers must abide by the following rules.

- Get **written permission** from the owner of the computer system and/or computer network before hacking.
- **Protect the privacy of the organization** been hacked.
- **Transparently report** all the identified weaknesses in the computer system to the organization.
- **Inform** hardware and software vendors of the **identified weaknesses**.

Cracker (Black hat): A hacker who gains unauthorized access to computer systems for personal gain. The intent is usually to steal corporate data, violate privacy rights, transfer funds from bank accounts etc.

Grey hat: A hacker who is in between ethical and black hat hackers. He/shebreaks into computer systems without authority with a view to identify weaknesses and reveal them to the system owner.

Script kiddies: A non-skilled person who gains access to computer systems using already made tools.

Hacktivist: A hacker who use hacking to send social, religious, and political, etc. messages. This is usually done byhijacking websites and leaving the message on the hijacked website.

Phreaker: A hacker who identifies and exploits weaknesses in telephones instead of computers.
Ethical Hacking is identifying weakness in computer systems and/or computer networks and coming withcountermeasures that protect the weaknesses.

Teenage Web Vandals-IT defines, vandalism as willful or malicious destruction, injury, disfigurement, or defacement of any public or private property, real or personal, without the consent of the owner or persons having custody or control. Vandalism includes a wide variety of acts, including graffiti, damaging property (smashing mailboxes, trashing empty buildings or school property, breaking windows, etc.), stealing street signs, arson, egging homes or cars, toilet papering homes, and other types of mischief.

Cyber Fraud and Cheating-It means the person who is doing the act of cyber-crime i.e. stealing password and data storage has done it with having guilty mind which leads to fraud and cheating.

Defamation-The offense of injuring a person's character, fame, or reputation by false and malicious statements. Any derogatory statement, which is designed to injure aperson's business or reputation, constitutes cyber defamation. Defamation can be accomplished as libel or slander. Cyber defamation 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 to all of that person's friends.

Harassment -Harassment is a form of discrimination. It involves any unwanted physical or verbal behaveor that offends or humiliates you. Generally, harassment is a behavior that persists over time. Serious one - time incidents can also sometimes be considered harassment.

E-mail Abuse-Email Abuse, also known as junk email, is a type of electronic spam where unsolicited messages are sent by email. Many email spam messages are commercial in nature but may also contain disguised links that appear to be for familiar websites but in fact lead to phishing web sites or sites that are hosting malware. Spam email may also include malware as scripts or other executable file attachments (Trojans).

Other IT Act Offences-The offences included in the IT Act 2000 are as follows:

- Tampering with the computer source documents.
- Hacking with computer system.
- Publishing of information which is obscene in electronic form.
- Power of Controller to give directions
- Directions of Controller to a subscriber to extend facilities to decrypt information
- Protected system
- Penalty for misrepresentation
- Penalty for breach of confidentiality and privacy
- Penalty for publishing Digital Signature Certificate false in certain particulars
- Publication for fraudulent purpose
- Act to apply for offence or contravention committed outside India
- Confiscation
- Penalties or confiscation not to interfere with other punishments.
- Power to investigate offences.

Monetary Penalties-A Monetary Penalty is a civil penalty imposed by a regulator for a contravention of an Act, regulation or by-law. It is issued upon discovery of an unlawful event, and is due and payable s subject only to any rights of review that may be available under the AMP's implementing scheme. It is regulatory in nature, rather than criminal, and is intended to secure compliance with a regulatory scheme, and it can be employed with the use of other administrative sanctions, such as demerit points and license suspensions.

Electronic Governance- In this era of computer where every word is getting prefixed by word 'E', Government of India is also not lacking behind and to provide its services to the citizens at their fingertips the Government is also turning in E- Governance. E-Governance is nothing but providing Government Services cheaper, faster and efficiently to thecitizens through internet and computer. The Information Technology Act, 2000 gives recognition to the Electronic Governance. Chapter III, Section 4 to Section 10-A, of the Act provides for the provisions regarding Electronic Governance. Section 4 and 5 gives Legal Recognition to electronic records and electronic signatures. Section 6 of the Act authenticates use of electronic record and electronic signatures in Government and its agencies. The aim electronic government is to ensure transparency in Government. It also makes the Government accessible to the citizen residing in the most remote village of the country.

Jurisdiction and Cyber Crimes:

Jurisdiction over Internet-The whole trouble with internet jurisdictionis the presence of multiple parties in various parts of the world who have only a virtual nexus with each other. Then, if one party wants to sue the other, where can he sue?

Traditional requirement generally encompass two areas: -

- The Place where the defendant reside.
- Where the cause of action arises.

However, in the context of the internet or cyberspace (Cyberspace is the electronic medium of computer networks, in which online communication takes place), both these are difficult to establish with any certainty. Considering the lack of physical boundaries on the internet, is it possible to reach out beyond the court's geographic boundaries to haul a defendant into its court forconduct in "Cyberspace"? Issues of this nature have contributed to the complete confusion and contradictions that plague judicial decisions in the area of internet jurisdiction. Accordingly, in each case, a determination should be made as to where an online presence will subject the user to jurisdiction in a distant state or a foreign company.

As such, a single transaction may involve the laws of at least three jurisdictions:

- The laws of the state/nation in which the user resides,
- The laws of the state/nation that apply where the server hosting the transaction is located.
- The laws of the state/nation which apply to the person or business with whom the transaction takes place.

Nature of Criminality- Human individuals as considered as the basis of explaining crime as an individual criminality. As compared to the theory of crime as a social construct, the focus of the concept of crime as an individual criminality is already on the individual. Rooting from the person, it looks into the innate or inherent factors that can significantly influence the making of a criminal.

Compounding of Offences

As per Section 77-A of the I. T. Act, any Court of competent jurisdiction may compound offences, other than offences for which the punishment for life or imprisonment for a term exceeding three years has been provided under the Act.

No offence shall be compounded if;

- The accused is, by reason of his previous conviction, is liable to either enhanced punishment or to the punishment of different kind; OR
- Offence affects the socio economic conditions of the country; OR
- Offence has been committed against a child below the age of 18 years; OR
- Offence has been committed against a woman.

The person accused of an offence under this Act may file an application for compounding in the Court in which offence is pending for trial and the provisions of Sections 265-B and 265-C of Cr. P. C. Shall apply.

In the perspective of individual criminality, it can be asserted that a criminal is born or can be made.

In the claim that a criminal is born, it can be traced on the studies regarding the importance of heredity. On the other hand, the claim that a criminal is made, it is traced on an individual's

environment - one's diet and even the environment. While, the aspect of environment is still included in the theory of individual criminality, it is still geared towards the study of theindividual.
The concept of a born criminal can be traced with the studies that show the importance and power of oneself in the development of one's criminality. Being a born criminal is also equated to being hereditary. A person is more likely to become criminal is it is already in their blood to become one. In heredity, it includes the elements like physical appearance, modern genetics theory as well as learning theory.

Strategies to tackle Cyber Crime and Trends:

- **Protect Your Most Visible Asset-**Websites are the most visible and vulnerable part of a company's infrastructure. As hackers scan the Internet nonstop in search of weaknesses, companies should not overlook this vulnerable entry point in their cyber security defense strategy. Products like malware and vulnerability scanners and web-application firewalls can help you guard this important asset that is the face of your brand.
- **Focus on Effects-** I t's clear that organizations can't prevent 100 percent of intrusions. A sophisticated and determined adversary will eventually get in. This is why companies should focus on detecting the effects (also called indicators of attack) of malware and adversary activity, and not just look out for known bad signatures (known as indicators of compromise.
- **Remember That People Are Your Weakest Link-**Even the most advanced technology can't prevent a great employee from accidentally opening your doors to cybercrime. Their strong, alphanumeric 32 - character password is now exposed in a plaintext email. These unintentional slip-ups happen; combat them by reiterating common sense practices to all of your employees.
- Prevention is always better than cure. It is always better to take certain precautions while working on the net. One should make them a part of his cyber life. Sailesh KumarZarkar, technical advisor and network security consultant to the Mumbai Police Cybercrime Cell, advocates the 5P mantra for online security: Precaution, Prevention, Protection, Preservation and Perseverance.
- Identification of exposures through education will assist responsible companies and firms to meet these challenges.
- One should avoid disclosing any personal information to strangers, the person whom they don t know, via e-mail or while chatting or any social networking site.
- One must avoid sending any photograph to strangers by online as misusing or modification of photograph incidents increasing day by day.
- An update Anti-virus software to guard against virus attacks should be used by all the netizens and should also keep back up volumes so that one may not suffer data loss in case of virus contamination.
- A person should never send his credit card number or debit card number to any site that is not secured, to guard against frauds.
- It is always the parents who have to keep a watch on the sites that their children are accessing, to prevent any kind of harassment or depravation in children.
