Overview

1. Need of cyber law
2. Cyber crime
3. Introduction of cyber law
   - IT act 2000
   - IT act amendment 2008
4. Cyber Law in world
5. Importance of cyber law in present era
Brief about Cyber law

“The modern thief can steal more with a computer than with a gun. Tomorrow’s extremist may do more damage with a keyboard than or with a bomb”

* Cyber space creates moral, civil and criminal wrongs. It has now given a new way to express criminal tendencies

* Information technologies is encompassing all walks of life all over the world

* Internet has dramatically changed the way we think, the way we govern, the way we do commerce and the way we perceive ourselves

*cyber space is open to participation by all

* It has brought transition from paper to paperless world
Cyber law

- Cyber law is the law governing cyber space
- Cyber space includes computers, networks, soft wards, data storage devices (such as hard disks, USB disks), the internet, websites, emails and even cell phones, ATM machines

- Cyber law deals with
  * Cyber crimes
  * Electronic or digital signatures
  * Intellectual properties
  * Data protection & privacy
Categories of cyber crime

- Cyber crime against persons
- Cyber crimes against property
- Cyber crimes against government

Against a person

* Cyber stalking
* Impersonation
* Loss of privacy
* Transmission of obscene material
* Harassment with the use of computer
Against Property

Un authorized computer trespassing

- Computer vandalism
- Transmission of harmful programmes
- Stealing secret information & data
- Copy rights

Against government

Some other crimes:

- Logic bombs
- Spamming

* Hacking government website
* Cyber extortion
* Cyber terrorism
* Computer viruses

- virus, worms, Trojan
  -email bombing
- E-mail abuse
The information technology act, 2000 (IT act) came into force on 17\textsuperscript{th} October 2000.

The primary purpose of the act is to provide legal recognition to electronic commerce and to facilitate filing of electronic records with the government.

Information technology act 2000 consisted of 94 sections segregated into 13 chapters.
IT Act -2000 Objectives

- To provide legal recognition for transactions
- To facilitate electronic filing of documents with the govt. agencies
- To amend the IPC, the Indian evidence act 1872, the bankers book evidence act 1891 and the reserve bank of India act 1934.
- Aims to provide the legal frame work to all electronic records
IT Act 2000—snap shot of important Cyber Law Provisions in India

- Section 43 - offence, tempering with computer source, documents (without permission of in-charge
- Sec-66 - Hacking with computer system, data alteration
- Sec-67 - Publishing obscene information
- Sec-70 - Unauthorized access to protected system
- Sec-72 - Breach of confidentiality & privacy
- Sec-73 – Publishing false digital signature certificates
- Sec-503 & 499 IPC – Sending threatening & defamatory messages by email
IT Act 2000-snap shot of important Cyber Law Provisions in India

- Sec-463 – Forgery of electronic records
- Sec-420 – Bogus websites, cyber fronds
- Sec-463 & 500 – Email spoofing & abuse
- Sec-383 – Web jacking
- NDPS Act – Online sale of drugs
- Arms Act- Online sale of Arms
The information technology amendment act 2008 has been passed by the parliament on 23rd December 2008

It received the assent of president of India on 5th February 2009

The IT act 2008 has been notified on 27th October 2009

IT act 2008 is a new version of IT act 2000

Provides additional focus on information security
IT Act Amendment 2008

- Added several new sections on offences including cyber terrorism & data protection
- 124 sections & 14 chapters
- Digital signature has been replaced with electronic signature
- Sec 67 of the old act is amended
- Amended Sec 69 gives power to the state
Importance of cyber law

- We are living in highly digital world
- All companies depend upon their computer networks & keep their valuable data in electronic form
- Govt. forms including income tax returns, company law forms etc., are now filled in electronic form
- Consumers are increasingly using credit cards for shopping
- Most people are using email, cell phone, SMS for communication
- Even in “non-cyber crime” cases also important evidence is found in computers/cell phones etc. in case of divorce, murder, kidnapping organized crime, terrorist operations.
A.P Government & Police Initiative
Cyber Safety for Women & Children

Cyber safety measures

➢ Never accept friends requests from unknown people on social media platforms

➢ Use caution when share personal information/emotions with virtual friends/chat room partners etc. whom you don’t know in your real life.

➢ Never share your passwords, credit/debit card PIN/OTP to anyone

➢ Disable camera permission and keep the lens of your camera closed or covered when not in use

➢ Always let your friends and family know where you are going and who you are meeting
- Disable geo tagging in your camera. Enable it only when required
- Always logout from online accounts when you are done
- Never click on a link from an un-trusted source
- Use safety tips like filtering emails, locking personal albums and information, personal walls of social networking sites etc.
- Use pseudo names instead of real names in internet
A.P Government & Police Initiative
Cyber Safety for Women & Child
Cyber safety measures

- Don’t share /forward abused messages/images/videos and rumours in internet
- Enable parental controls on systems and gaming consoles to manage child’s online activities
- Avoid using free, unsecured Wi-Fi for shopping or banking on the internet and even for logging into your media profiles
- Keep evidence of bullying behavior such as instant messenger conversations or online posts
- Avoid saving your credit/debit cards information on websites, web browsers and gaming sites
A.P Government & Police Initiative
Cyber Safety for Women & Child
Cyber safety measures

- Security updates and pitches keep the latest threats away. Always install them no matter how busy you are.
- Don’t mail back to unknown senders of spam/ pornographic/ erotic/ phishing.
- Freebies come as games, offers, deals, etc. they may be riddled with viruses, spyware and malicious software.
- Familiarize yourself with blocking and reporting functions in social media sites.
- Go for unique and hard to guess password.
- Report to law enforcement agencies if you find any viral scare in online.
- Enable privacy options and two-factor authentication on social media sites.
- Don’t mail back to unknown senders of spam/ pornographic/ erotic/ phishing.
A.P Government & Police Initiative
Cyber Safety for Women & Child
Cyber safety measures

- Report to law enforcement agencies if you find any viral scare in online
- Enable privacy options and two-factor authentication on social media sites
- For enabling/disabling privacy settings in social media
  - Facebook: https://www.facebook.com/help/325807937506242
  - Instagram: https://help.instagram.com/196883487377501
Connect us on

https://www.facebook.com/vmmngo

https://twitter.com/vmmngo

https://www.instagram.com/vasavyamahilamandali/

https://vmmstories.blogspot.com/

https://www.youtube.com/VasavyaMahilaMandaliNGO

https://www.linkedin.com/in/vasavya-mahila-mandali-966272167
Thank you