Unit 3

↗ course	📙 [Constitution of India, Cyber Law and Professional Ethics](#)
⟳ mastery	none
⟳ progress	not started

Unit 3 - Cyber Laws

- Cyber laws → related to computer technology

- Any illegal behaviour committed by means of/in relation to a computer or network → cyber crime

- Information Technology Act, 2000 (amended in 2008) - provides legal recognition to e-commerce and facilitates filing of electronic records with the govt.

  - Legal recognition of e-documents

  - Legal recognition of e-signatures

  - Offenses and contraventions (punishments prescribed for the offense in question)

  - Justice dispensation systems for cyber crimes

Identity Theft/Email Spoofing

- Sending messages while impersonating someone else

- Origin is different from that where it seems to come from

- 66C of IT Act: Using someone else's password/e-signature to commit fraud etc → 3 years imprisonment (or) fine of 1L rupees (or) both

Eg: Creating accounts on social media pretending to be someone else

Hacking

- Also denoted as "unauthorised access"; but note that IT Act gives hacking a more specific meaning and thus these terms should not be confused

- Includes Internet time theft (gaining access to the Internet using another person's network without their knowledge

- 66 of IT Act: Hacking → 3 years imprisonment (or) fine of 5L rupees (or) both

Eg: Bangladesh Bank heist (2016), Facebook (2018)

Denied Service Attack

- User of a website/service is denied from using the server or website

- Attackers send a large number of requests to the web server of the website under attack and overloads its maximum bandwidth ⇒ website slows down/crashes

Eg: 15 year old hacker "Mafiaboy" took down the servers of CNN, Dell, E-Trade, eBay, Yahoo in 2000

Mail Bombing

- Similar to denied service attack; attacker sends large volume of mail to some target address

- Email address (in case of a user) or mail server (in case of company/service provider) crashes

Virus Attack

- Viruses → Self duplicating programs that mount themselves without user approval → When executed, replicates and implants replicas of itself in data files of other programs/boot sector of hard drive

- Effects of virus attack:
  - Stealing hard disk space/CPU time
  - Retrieving private information
  - Corrupting data
  - Displaying radical messages on user's computers
  - Spamming links
  - Logging keystrokes
  - Trojan Horse attack

- Penalties under law:
    - Section 66: Refer Hacking
    - Section 43: Whoever without the permission of the person in-charge of the computer system accesses, downloads any data, introduces computer virus, causes denial of access → a penalty upto rupees one crore

Cyber Warfare

- Use of computer tech to disrupt the activities of a state/organisation by disabling financial and organisational systems. This is done by stealing/altering classified data to undermine networks, websites, services through viruses, Denial of Service attacks etc.
- All cyber wars are cyber crimes; all cyber crimes are not cyber wars
- Methods:
    - Espionage, national security breaches
    - Malwares, Denial of Service attacks, hacking etc.
- Cyber crime → politically motivated, destroys data/causes damage to infrastructure of specific country → Cyber war
- Same intentions as a military war between nation-states, but by using cyberspace instead

Cyber Terrorism

- Using computer tech to engage in terrorism
- Cyber terrorism → International concern
  Cyber crime → Domestic concern
- Common forms:
    - Dispersed/Widespread denial of service attacks
    - Hate websites/hate mails
    - Attacks on delicate computer networks
- 66F, IT Act: Cyber terrorism → Imprisonment upto life

Eg: Osama bin Laden; LITE attack on America's deployment system during Iraq war

Phishing

- Target contacted through electronic means by someone posing as a legitimate institution to lure them into leaking sensitive data

- Methods:

    - Fake websites

    - Wifi access points

    - Pop ups on websites

- Penalties under law:

    - Section 43: Refer Virus Attack

    - Section 66: Refer Hacking

    - Section 66A: Sending offensive messages → Imprisonment up to three years and with fine
      NOTE: Section 66A has been struck down by Supreme Court's Order dated 24th March, 2015 in [Shreya Singhal vs. Union of India](#)

    - Section 66C: Refer Identity Theft

    - Section 66D: Cheating/fraud using computer tech → Imprisonment up to three years, or/and with fine up to ₹1,00,000

Bandwidth Theft/Hotlinking

- Bandwidth → Amount of data transferred from a website to a user's computer

- If a site is over its monthly bandwidth, it's billed for the extra data or taken offline

- Bandwidth theft/hotlinking → Using images/files from someone else's website by directly linking them on your site

- Penalties under law:

    - Section 43: Refer Virus Attack