COMPUTING AND ETHICS

The four primary ethical and legal issues in computing are :-

- ✓ Accuracy
- ✓ Property- Identification and protection of rights.
- ✓ Access- Control of the access of the information.

- INTELLECTUAL PROPERTY RIGHTS

Intellectual property (IP) refers to creation of designs, concepts, software, inventions, formulas etc. It is protected by copyright, Trademark, and other legal measures.

Intellectual property rights are the rights over intellectual properties that allows the user to benefit from their own creation. The world intellectual property organization ensures the rights of creators and owners of intellectual property.

- COPYRIGHT

Copyright is the right of authors, artists and other creators for their creations. The creations include novels, poems, plays etc.

- TRADEMARK

A trademark is a distinctive sign that identifies and distinguishes a product or service provider by an individual and a company. It is also referred to as Logo. The Trademark can be words like, phrases, symbols, designs, or a combination of these.

- PATENTS

A patent is an exclusive right grants the inventor of a product or process the right to manufacture, use or sell the product.

The other forms of intellectual property include:-

- ✓ Industrial Design
- ✓ Geographical indication

- PROTECTION OF INDIVIDUAL RIGHT TO PRIVACY

The right to privacy refers to the concept that an individual's personal information is protected from public scrutiny. It ensures:-

- ✓ Information privacy or Data protection – Involves rules for collecting and handling personal data.
- ✓ Bodily privacy – Involves protection of the physical protection of the body.
- ✓ Communication privacy – Involves privacy of the individuals communication through telephone calls, E-mail etc.
- ✓ Territorial Privacy – Involves setting up limits on intrusion through methods such as searches, public surveillance, etc.

- DATA PROTECTION ON INTERNET

Data protection is defined as the law designed to protect personal data, the laws ensure that the personal data is:-

- ✓ Obtained fairly and lawfully.
- ✓ Kept safe and secure.
- ✓ Kept accurate, complete and up to date.
- ✓ No longer for a specified purpose.
- ✓ Protection against spam, software privacy, cybercrime, hacking.

- SPAM

Spam is defined as irrelevant or unsolicited messages sent over the internet typically to a large number users for the purpose of advertising, phishing, spread malware.

- SOFTWARE PIRACY

The unauthorized copying of software is referred to as software piracy. The software programming ideas and methods can be stolen and the same code can be reused illegally.

- CYBER CRIME

  The cybercrime activities include planting:-

  - ✓ Computer virus, Storing photographic images and all sorts of activities.
  - ✓ Credit card fraud to multinational money laundering schemes. These activities can be done by fraudulent traders, hackers and terrorists.

- HACKING

  Hacking is defined as unauthorized access to data held on computer system. It is often caused by employees of a company who have inside knowledge of particular users and passwords. The motive behind hacking can often be mischievous. Hacking can be done for the purpose of:-

  - ✓ Theft of money.
  - ✓ Theft of data.
  - ✓ Fraud on the internet.

- STEPS TO PREVENT SPAMMING
  - ✓ Install spam filtering software's.
  - ✓ If you suspect that an e-mail is spam do not respond,just delete it.
  - ✓ Keep the software and security updates up to date.
- STEPS TO PREVENT SOFTWARE PIRACY
  - ✓ Buy the license to copy of software. Never make copies and circulate them.
  - ✓ Purchase software CD's from a reputed seller.
  - ✓ Avoid using illegal CD's.
  - ✓ If software is available online, download it directly from the manufacturers website.
- STEPS TO PREVENT HACKING
  - ✓ Keep your passwords secrets and change them periodically.

- ✓ Update your antivirus software's frequently..
- ✓ Never store your credit card information on a website.

- PROTECTION AGAINST MALICOS INTENT AND MALICIOUS CODE
  - ✓ A malicious code is referred to any code that is intended to cause undesired effects or damage to a system.
  - ✓ It can take the form of java applets, scripting languages, browser budget's etc.
  - ✓ It can cause the network and the ,main server overloaded by sending e-mail messages or files.
- VIRUS
  - ✓ Virus stands for vital information resources under seize.
  - ✓ Viruses' are generally developed with an intention to damage computer files.
  - ✓ When aninfected program is executed the virus spreads to other parts of the system.
  - ✓ Some viruses gets triggered when a particular application gets activated.
  - ✓ Example:- Friday 13^{th} VIRUS.
- INTERNAL THREATS TO A COMPUTER SYSTEM
  - ✓ Hardware failure:- When a hard disk crashes the contents of the hard disk becomes unreadable.
  - ✓ Fault procedure:- When an untrained employee, makes an entry into an account system it can cause havoc.
  - ✓ Natural disasters:- Fire, flood, hurricanes and earthquakes can destroy a building.
  - ✓ Negligence of users:- When employees neglect to take back of the data it can cause damage to their computers.
  - ✓ Dishonest staff:- Computer systems are vulnerable to fraud and theft of data both from inside and outside the organization.
- EXTERNAL THREATS TO A COMPUTER SYSTEM

- ✓ Hackers gain entry to company's data bases and can steal or corrupt the data.
- ✓ Download viruses from the internet.

- PROTECTION OF COMPUTER SYSTEM FROM ILLEGAL ACCESS
  - ✓ Measures that can be included are:-
    - ➢ Physical restrictions to the computer department – employees of the organization are requested to wear the ID card to restrict the access.
    - ➢ User name and Password:- When using a computer system, people are required to sign on with their user ID card and Password.
    - ➢ Data access and control;- Any data in the database can have restrictions by setting appropriate access rights.
    - ➢ Special software:- It can be installed on a computer system to maintain and audit of who has logged - in and for how much time.
    - ➢ Data encryption:- It is the process of converting the plain-text into an encryption code, to make the code impossible to track.
- GOOD ETHICS AND ETHICAL PRATISES
  - ✓ You should not use computer to steal information.
  - ✓ You should not use a computer to spread wrong information.
  - ✓ You should not use other people's computer resources without their authorization.
  - ✓ You should not use computer to steal.
- THE MAIN PRINCIPLES OF SOCIAL MEDIA ETHICS

  The main principles of social media ethics are:-
  - ✓ Authenticity
  - ✓ Transparency
  - ✓ Communication

- ACCESS TO INTERNET
  - ✓ Access to internet can be done using a proxy server.
  - ✓ A proxy server is a server that sits between a client application, such as a web browser and a real server.
  - ✓ It intercepts all request to the real server to see if it can fulfill the request itself. If not it forwards request to the real server.