Ch-11 Notes:

Intro: Most of our services rely on Internet today. And with the advancement in technology everyone can access, internet. So the intention of this chapter is to learn about the rights/morals etc.. about the internet world.

=========================

1. Digital Foot printing:

========================

Whenever we surf the Internet using smartphones, tablets, computers, etc., we leave a trail of data reflecting the activities performed by us online, which is our digital footprint.

Our digital footprint can be created and used with or without our knowledge.
Such data could be used for targeted advertisement or could also be misused or exploited. Thus, it is good to be aware of the data trail we might be leaving behind. This awareness should make us cautious about what we write, upload or download or even browse online.

Active digital footprints which includes data that we intentionally submit online. This would include emails we write, or responses or posts we make on different websites or mobile Apps, etc.

The digital data trail we leave online unintentionally is called passive digital footprints. This includes the data generated when we visit a website, use a mobile App, browse Internet, etc.

==============================

2. Digital Society and netizen

==============================

Anyone who uses digital technology along with Internet is a digital citizen or a netizen. Being a good netizen means practicing safe, ethical and legal use of digital technology. A responsible netizen must abide by net etiquettes, communication etiquettes and social media etiquettes.

2.1 Net Etiquettes

- Be Ethical
    - No copyright violation:
    - Share the expertise:
- Be Respectful
    - Respect privacy:
    - Respect diversity:
- Be Responsible
    - Avoid cyber bullying:
    - Don’t feed the troll:

2.2 Communication Etiquettes

- Be Precise
    - Respect time:

  - Respect data limits:
- Be Polite
  - we should be polite and non-aggressive in our communication. We should avoid being abusive even if we don’t agree with others’ point of view.
- Be Credible
  - We should be cautious while making a comment, replying or writing an email or forum post as such acts decide our credibility over a period of time.

2.3 Social Media Etiquettes

- Be Secure
  - Choose password wisely:
  - Know who you befriend:
  - Beware of fake information:
- Be Reliable
  - Think before uploading

3. Data Protection

Data or information protection is mainly about the privacy of data stored digitally.

Elements of data that can cause substantial harm, embarrassment, inconvenience and unfairness to an individual, if breached or compromised, is called sensitive data. Examples of sensitive data include biometric information, health information, financial information, or other personal documents, images or audios or videos.

Privacy of sensitive data can be implemented by encryption, authentication, and other secure methods to ensure that such data is accessible only to the authorised user and is for a legitimate purpose.

Each country has its own data protection policies (laws). These policies provide guidelines to the user on processing, storage and transmission of sensitive information. The motive behind implementation of these policies is to ensure that sensitive information is appropriately protected from modification or disclosure.

3.1 Intellectual Property Right (IPR)

Intellectual Property refers to the inventions, literary and artistic expressions, designs and symbols, names and logos. The ownership of such concepts lies with the creator. This enables the creator to earn recognition or financial benefit by using their creation or invention. Intellectual Property is legally protected through copyrights, patents, trademarks, etc.

- Copyright:

Copyright grants legal rights to creators for their original works like writing, photograph, audio recordings, video, sculptures, architectural works, computer software, and other creative works like literary and artistic work.

The rights include right to copy (reproduce) a work, right to create derivative works based upon it, right to distribute copies of the work to the public, and right to publicly display or perform the work. It prevents others from copying, using or selling the work.

- Patent

A patent is usually granted for inventions. Unlike copyright, the inventor needs to apply (file) for patenting the invention. When a patent is granted, the owner gets an exclusive right to prevent others from using, selling, or distributing the protected invention. Patent gives full control to the owner to decide whether or how the invention can be used by others.

A patent protects an invention for 20 years, after which it can be freely used.

- Trademark

Trademark includes any visual symbol, word, name, design, slogan, label, etc., that distinguishes the brand or commercial enterprise, from other brands or commercial enterprises.

For example, no company other than Nike can use the Nike brand to sell shoes or clothes.

3.2 Violation of IPR

Violation of intellectual property right may happen in one of the following ways:

- Plagiarism:

Presenting someone else’s idea or work as one’s own idea or work is called plagiarism. If we copy some contents from Internet, but do not mention the source or the original creator, then it is considered as an act of plagiarism.

- Copyright Infringement

Copyright infringement is when we use other person’s work without obtaining their permission to use or we have not paid for it, if it is being sold.
Suppose we download an image from the Internet and use it in our project. But if the owner of the copyright of the image does not permit its free usage, then using such an image even after giving reference of the image in our project is a violation of copyright

- Trademark Infringement

Trademark Infringement means unauthorised use of other’s trademark on products and services. An owner of a trademark may commence legal proceedings against someone who infringes its registered trademark.

3.3 Public Access and Open Source Software

Copyright sometimes put restriction on the usage of the copyrighted works by anyone else rather than completely stopping others to use it.

Licenses provide rules and guidelines for others to use the existing work. When authors share their copyrighted works with others under public license, it allows others to use and even modify the content. Open source licenses help others to contribute to existing work or project without seeking special individual permission to do so. The GNU General public license (GPL) and the Creative Commons (CC) are two popular categories of public licenses.

Creative Commons (CC) licenses are a set of copyright licenses that give the recipients, rights to copy, modify and redistribute the creative material, but giving the authors, the liberty to decide the conditions of licensing.

General public license (GPL) is the most widely used free software license which grants the recipients, rights to copy, modify and redistribute the software and that the same rights are preserved in all derivative works.

Many of the proprietary software that we use are sold commercially and their program code (source code) are not shared or distributed. However, there are certain software available freely for anyone and their source code is also open for anyone to access, modify, correct and improve.

Free and open source software (FOSS) has a large community of users and developers who are contributing continuously towards adding new features or improving the existing features. Some of the popular FOSS tools are Linux based operating System like Ubuntu, office packages, like Libre Office, browser like Mozilla Firefox, etc.

Software piracy is the unauthorised use or distribution of software. Those who purchase a license for a copy of the software do not have the rights to make additional copies without the permission of the copyright owner. One should avoid software piracy. Using a pirated software not only degrades the performance of a computer system, but also affects the software industry which in turn affects the economy of a country.

4. Cyber Crime

Cyber Crime is defined as a crime in which computer is the medium of crime (hacking, phishing, spamming), or the computer is used as a tool to commit crimes (extortion, data breaches, theft).

4.1 Hacking

Hacking is the act of unauthorised access to a computer, computer network or any digital system.

Hacking, when done with a positive intent, is called ethical hacking. Such ethical hackers are known as white hat hackers.
They are specialists in exploring any vulnerability or loophole during testing of the software. Thus, they help in improving the security of a software. Ethical hacking is actually preparing the owner against any cyber-attack.

A non-ethical hacker is the one who tries to gain unauthorised access to computers or networks in order to steal sensitive data with the intent to damage or bring down systems. They are called black hat hackers or crackers.
Their primary focus is on security cracking and data stealing. They use their skill for illegal or malicious purposes.

4.2 Phishing and Fraud Emails

Phishing is an unlawful activity where fake websites or emails that look original or authentic are presented to the user to fraudulently collect sensitive and personal details like usernames, passwords, banking and credit card details.

The most common phishing method is through email spoofing. They send email from an address that looks similar to your bank or educational institution, asking for your information, but if you look carefully you will see their URL address is fake.
They will often use logos of the original, making them difficult to detect from the real! Phishing attempts through phone calls or text messages are also common these days.

- Identity Theft:

Identity thieves increasingly use personal information stolen from computers or computer networks, to commit fraud by using the data gained unlawfully.
A user’s identifiable personal data like demographic details, email ID, banking credentials, passport, PAN, Aadhaar number and various such personal data are stolen and misused by the hacker on behalf of the victim.
They use this data to take advantage of an individual’s stolen identity. Given below are a few examples:

- Financial identity theft: when the stolen identity is used for financial gain.
- Criminal identity theft: criminals use a victim’s stolen identity to avoid detection of their true identity.
- Medical identity theft: criminals can seek medical drugs or treatment using a stolen identity.

4.3 Ransomware

This is another kind of cyber crime where the attacker gains access to the computer and blocks the user from accessing, usually by encrypting the data.
The attacker blackmails the victim to pay for getting access to the data, or sometimes threaten to publish personal and sensitive information or photographs unless a ransom is paid.

4.4 Combatting and Preventing Cyber Crime

Following points can be considered as safety measures to reduce the risk of cyber crime:

- Take regular backup of important data
- Use an antivirus software and keep it updated always
- Avoid installing pirated software. Always download software from known and secure (HTTPS) sites
- Always update the system software which include the Internet browser and other application software

- Do not visit or download anything from untrusted websites
- Usually the browser alerts users about doubtful websites whose security certificate could not be verified; avoid visiting such sites
- Use strong password for web login, and change it periodically. Do not use same password for all the websites. Use different combinations of alphanumeric characters including special characters. Ignore common words or names in password
- While using someone else's computer, don't allow browser to save password or auto fill data, and try to browse in your private browser window
- For an unknown site, do not agree to use cookies when asked for, through a Yes/No option.
- Perform online transaction like shopping, ticketing, and other such services only through well-known and secure sites
- Always secure wireless network at home with strong password and regularly change it.

==

5. Indian Information Technology act (IT Act)

==

The Government of India's Information Technology Act, 2000 (also known as IT Act), amended in 2008, provides guidelines to the user on the processing, storage and transmission of sensitive information.

In many Indian states, there are cyber cells in police stations where one can report any cyber crime. The act provides legal framework for electronic governance by giving recognition to electronic records and digital signatures. The act outlines cyber crimes and penalties for them.

Cyber Appellate Tribunal has been established to resolve disputes arising from cyber crime, such as tampering with computer source documents, hacking the computer system, using password of another person, publishing sensitive personal data of others without their consent, etc.

The act is needed so that people can perform transactions over the Internet through credit cards without fear of misuse. Not only people, the act empowers government departments also to accept filing, creation and storage of official documents in the digital format.

====================

6. Impact on health

====================

With the advancement in technology we are spending more time in front of screens, be it mobile, laptop, desktop, television, gaming console etc.

But interacting in an improper posture can be bad for us — both physically, and mentally. Besides, spending too much time on Internet can be addictive and can have a negative impact on our physical and psychological well being.
Stress, physical fatigue and obesity are the other related impacts the body may face if one spends too much time using digital devices.

However, these health concerns can be addressed to some extent by taking care of the way we position such devices and the way we position our posture.

Ergonomics is a branch of science that deals with designing or arranging workplaces including the furniture, equipments and systems so that it becomes safe and comfortable for the user. Ergonomics helps us in reducing the strain on our bodies — including the fatigue and injuries due to prolonged use.