CHAPTER 17: SOCIETY LAW AND ETHICS

Cyber crimes is one of the most threatening terms that is an evolving phase. It is said that major percentage of the World War III will be based on cyber-attacks by cyber armies of different countries.

Cyber crime can be categorized into 2 types. These are peer-to-peer attack and computer as weapon. In peer-to-peer attack, attackers target the victim users; and in computer as weapon attack technique, computers are used by attackers for a mass attack such as illegal and banned photo leak, IPR violation, pornography, cyber terrorism etc.

Cyber-criminals are involved in activities like accessing online accounts in unauthorized manner; use Trojans to attack large systems, sending spoofed emails. But cyber-criminals do not report any bug is found in a system, rather they exploit the bug for their profit.

Cyber-laws were incorporated in our law book not only to punish cyber criminals but to reduce cyber crimes and tie the hands of citizens from doing illicit digital acts that harm or damage other's digital property or identity.

The Indian legislature thought of adding a chapter that is dedicated to cyber law. This finally brought India's Information Technology (IT) Act, 2000 which deals with the different cyber-crimes and their associated laws.

Under section 66 of IT Act, 2000 which later came up with a much broader and precise law says that cracking or illegally hacking into any victim's computer is a crime. It covers a wide range of cyber-crimes under this section of the IT Act.

DDoS (Distributed Denial of Service), IPR violation, pornography are mass attacks done using a computer. Spying someone using keylogger is an example of peer-to-peer attack.

HOTS BASED QUESTIONS :

1. What are intellectual propery rights ?
2. What is Plagiarism?
3. What is open source softwares ?
4. What are the privacy laws in IT ?
5. What is Cyber Crime and cyber security ?
6. What is the difference between Phishing and Vishing ?
7. What is illegal download ? What are the method to avoid it ?
8. What is child pornography?
9. What do you mean by cyber scam and how to avoid it ?
10. What is W-waste management ?
11. What are the biometrics devices? What do you mean by internet as an echo chamber ?

ANSWERS : SOCITY LAW AND ETHICS

1. **Intellectual property rights** are the **rights** given to persons over the creations of their minds. They usually give the creator an exclusive **right** over the use of his/her creation for a certain period of time12.

2. **Plagiarism** is the "wrongful appropriation" and "stealing and publication" of another author's "language, thoughts, ideas, or expressions" and the representation of them as one's own original work. **Plagiarism** is considered academic dishonesty and a breach of journalistic ethics.

3. Open-source software is a type of computer software in which source code is released under a license in which the copyright holder grants users the rights to study, change, and distribute the software to anyone and for any purpose. Open-source software may be developed in a collaborative public manner.

4. Privacy law refers to the laws that deal with the regulation, storing, and using of personally identifiable information of individuals, which can be collected by governments, public or private organisations, or other individuals.

   Privacy laws are considered within the context of an individual's privacy rights or within reasonable expectation of privacy.

5. The **crime** that involves and uses computer devices and Internet, is known as **cybercrime**. **Cybercrime** can be committed against an individual or a group; it can also be committed against government and private organizations. It may be intended to harm someone's reputation, physical harm, or even mental harm.

6. Voice **phishing**, or "**vishing**", works the same way as a spear **phishing** attack (by using personalized information to leverage trust), but uses a different channel: the telephone. The scammer calls an individual, pretending to be calling for a trusted organization (like the bank or your credit card company).

7. *Illegal downloading* places your computer at high risk of receiving viruses. Most *illegal downloading* is done through Peer-to-Peer (P2P) software, which allows people to share their files with others.

1. Remove the Incentive

One of the most-effective ways of dealing with piracy is by removing the incentive for the consumers to look for pirated content. Effectively this can be characterised by offering a good product and a good user experience at a fair price. Price is not the only differentiator. The importance of the user experience cannot be understated; viewers want sympathetic interfaces that contain the usual sophisticated bells and whistles such as personal recommendations, and they want excellent picture quality with no buffering and/or latency. The more the industry can provide that at realistic cost, the less people will be driven towards pirate arms.

You are not going to stop everyone from watching pirated content, but this can definitely remove some of the more casual illegal consumers.

2. PR & Education

There are several strands to this, but effectively the goal is to highlight to the consumer that piracy is a crime and it is illegal. To those within the industry this is obvious; to those outside it, it is anything but.

We've written recently of the problem of password sharing and how up to 42% of GenZ viewers are sharing log-in credentials. This has become a normative crime — one that 'everyone' does and so the activity no longer appears as illegal because the behaviour is normal. The usual example given is speeding, but video piracy is prevalent enough that maybe it should replace speeding in the textbooks. Efforts made to remind viewers that piracy is both morally wrong and a crime can prove successful in driving down numbers, as have been campaigns that have highlighted the role of organised crime in pirate activities, exposure to malware and inappropriate material, and the danger to advertisers of negative brand association with pirate sites.

3. Barriers to Entry

In the same way that you want to make it easy for consumers to choose legal alternatives, you want to make it hard for the pirates. The era of unprotected content is long gone. Content owners look to protect their investment and Intellectual Property, and will only strike licensing deals with operators that can demonstrate that they take such threats to the revenue stream seriously in turn.

What that means in practice, is changing all the time. Where once card-based Conditional Access Systems were as sophisticated as operators could get, the move towards IP and OTT delivery has necessitated a transition to software-based Digital Rights Management in turn. Even so, there is no single technology that can guarantee security. The best practice now involves a multi-disciplinary approach that encompasses both prophylactic anti-piracy measures and the following two criteria governing detection and enforcement as well.

4. Technology & Operations

You can't fight ghosts; you need to know what content is being pirated and where. That means being able to identify content, a live pirate stream as having come from your own video ecosystem. That requires technical intervention at the pre-transmission stage. Monitoring is the key to success here, whether automated — and there are some interesting developments in AI monitoring of video streams, both deployed and under development — or human-led. In an ideal world, at least for now, a hybrid solution is typically deployed.

Once a breach has been detected, swift action is necessary to deal with it. This has become ever-more important in recent years as piracy has pivoted towards realtime streaming and the lucrative illegal revenue streams associated with live sport in particular (the premium prices paid for accessing sports content making it a particular target).

Here, high-level agreements with the search engines and social networks consumers use to locate pirated content are key to rapid and realtime action.

5. Legal & Enforcement

There are a variety of countermeasures that TV Service Providers can use to interrupt and remove pirated content, from the traditional take-down notices to increasingly sophisticated realtime messages. With the correct anti-piracy services, operators can identify consumers who are watching illegal streams and incentivize them switch to legitimate services. These actions scale from soft to hard, with the harder countermeasures involving the introduction of law enforcement authorities.

The key is speed. While prosecution will always be a much slower process that happens after the event, removing the content from the internet as swiftly as possible is the best way to deter pirates and drive consumers towards legal alternatives.

6. Cooperation

While companies at all levels of the broadcast chain are used to competition, the losses to content piracy are too great for there not to be concerted efforts at cooperation. These need to take place at all levels of the industry and at all steps of the process, from production and on-set content security through to transmission.

The concept of herd immunity that is such a crucial aspect of global vaccination programs is important here. The more companies and organisations that are involved, the more effective the overall solution. Unfortunately the converse can also be true, and if there is any weak spot in the chain at any point, even in a place far removed from what was considered to be the primary route to the consumer's television or device, that weakness is there to be exploited.

8. *child pornography* means

(a) a photographic, film, video or other visual representation, whether or not it was made by electronic or mechanical means,

- (i) that shows a person who is or is depicted as being under the age of eighteen years and is engaged in or is depicted as engaged in explicit sexual activity, or
- (ii) the dominant characteristic of which is the depiction, for a sexual purpose, of a sexual organ or the anal region of a person under the age of eighteen years;

(b) any written material, visual representation or audio recording that advocates or counsels sexual activity with a person under the age of eighteen years that would be an offence under this Act;
(c) any written material whose dominant characteristic is the description, for a sexual purpose, of sexual activity with a person under the age of eighteen years that would be an offence under this Act; or
(d) any audio recording that has as its dominant characteristic the description, presentation or representation, for a sexual purpose, of sexual activity with a person under the age of eighteen years that would be an offence under this Act.

9. Cybercriminals are constantly looking for ways to make money at your expense. Individuals and organisations often fall prey to frauds that involve various forms of social engineering techniques, where the information required is garnered from a person rather than breaking into a system.

   These scams are typical examples of how cyber attackers can easily play on people's psychology and perceptions. The tips provided here are aimed to help you protect yourself. Awareness is your best defence!

GENERAL TIPS:

- Check your online accounts regularly.
- Check your bank account regularly and report any suspicious activity to your bank.
- Perform online payments only on secure websites (check the URL bar for the padlock and https) and using secure connections (choose a mobile network instead of public Wi-Fi).
- Your bank will never ask you for sensitive information such as your online account credentials over the phone or email.
- If an offer sounds too good to be true, it's almost always a scam.
- Keep your personal information safe and secure.
- Be very careful about how much personal information you share on social network sites. Fraudsters can use your information and pictures to create a fake identity or to target you with a scam.
- If you think that you have provided your account details to a scammer, contact your bank immediately.
- Always report any suspected fraud attempt to the police, even if you did not fall victim to the scam.

10. *Waste management* (or *waste disposal*) are the activities and actions required to *manage waste* from its inception to its final *disposal*. This includes the *collection*, transport, *treatment* and *disposal* of *waste*, together *with* monitoring and regulation of the *waste management* process.

11. A **biometric device** is a security identification and authentication **device**. Such **devices** use automated methods of verifying or recognising the identity of a living person based on a physiological or behavioral characteristic. These characteristics include fingerprints, facial images, iris and voice recognition.

    echo chamber refers to the overall phenomenon by which individuals are exposed only to information from like-minded individuals, while filter bubbles are a result of algorithms that choose content based on previous **online** behavior, as with search histories or **online** shopping activity.