Qn No 2:

Cyber Law

Cyber law also called IT law is the law regarding Information-technology including computers and internet. It is related to legal informatics and supervises the digital circulation of information, software, information security and e-commerce

Area of Cyber Law

The major areas of cyber law include :

Fraud : Consumers depend on cyber laws to protect them from online fraud. Laws are made to prevent identity theft, credit card theft and other financial crimes that happen online. A person who commits identity theft may face confederate or state criminal charges. They might also encounter a civil action brought by a victim. Cyber lawyers work to both defend and prosecute against allegations of fraud using the internet.

Copyright : The internet has made copyright violations easier. In early days of online communication, copyright violations were too easy. Both companies and individuals need lawyers to bring actions to impose copyright protections. Copyright violation is an area of cyber law that protects the rights of individuals and companies to profit from their own creative works.

Defamation : Several personnel use the internet to speak their mind. When people use the internet to say things that are not true, it can cross the line into defamation. Defamation laws are civil laws that save individuals from fake public statements that can harm a business or someone's personal reputation. When people use the internet to make statements that violate civil laws, it is called defamation law.

Harassment and Stalking : Sometimes online statements can violate criminal laws that forbid harassment and stalking. When a person makes threatening statements again and again about someone else online, there is violation of both civil and criminal laws. Cyber lawyers both prosecute and defend people when stalking occurs using the internet and other forms of electronic communication.

Freedom of Speech : Freedom of speech is an important area of cyber law. Even though cyber laws forbid certain behaviors online, freedom of speech laws also allow people to speak their minds. Cyber lawyers must advise their clients on the limits of free speech including laws that prohibit obscenity. Cyber lawyers may also defend their clients when there is a debate about whether their actions consist of permissible free speech.

Trade Secrets : Companies doing businesses online often depend on cyber laws to protect their trade secrets. For example, Google and other online search engines spend lots of time developing the algorithms that produce search results. They also spend a great deal of time developing other features like maps, intelligent assistance and flight search services to name a few. Cyber laws help these companies to take legal action as necessary in order to protect their trade secrets.

Contracts and Employment Law : Every time you click a button that says you agree to the terms and conditions of using a website, you have used cyber law. There are terms and conditions for every website that are somehow related to privacy concerns

<u>Protection Measures</u>

Use strong passwords : This can't be emphasized enough. If you have "qwerty123" as your bank's password and a lot of money in the account, you must be ready for a surprise transaction. You should not fully rely on the rate-limiting measures used by websites that you visit. Your password should be strong enough to be practically unbreakable. A strong password is one that is 12+ characters long and contains a diverse use of alphabets (both cases), numbers and symbols (and spaces). Setting a really unbreakable password should not be difficult specially when there are help available as random password generators. You can use this one or this one.

Keep your software up-to-date : Despite the developer's best intention to create secure software and thorough reviews from the security teams, there are unfortunately many zero-days that are revealed once the software is being used by a large user base. Companies are well aware of this fact and that is why they release frequent updates to patch these vulnerabilities. This is the reason why those updates, however annoying they may be, are important. They help in preventing attacks that can easily skip the radar of the antivirus programs on your computer.

Avoid identity theft : Identity theft is when someone else uses your personal information to impersonate you on any platform to gain benefits in your name while the bills are addressed for you. It's just an example, identity theft can cause you to damage more serious than financial losses.

The most common reason for identity theft is improper management of sensitive personal data. There are some things to be avoided when dealing with personally identifiable data :

- Never share your Aadhar/PAN number (In India) with anyone whom you do not know/trust.
- Never share your SSN (In US) with anyone whom you do not know/trust.
- Do not post sensitive data on social networking sites.
- Do not make all the personal information on your social media accounts public.
- Please never share an Aadhar OTP received on your phone with someone over a call.
- Make sure that you do not receive unnecessary OTP SMS about Aadhar (if you do, your Aadhar number is already in the wrong hands)
- Do not fill personal data on the website that claim to offer benefits in return.