FRANCIS XAVIER ENGINEERING COLLEGE
AUTONOMOUS INSTITUTION
ACCREDITED BY NBA

UNIT 4 – QUESTION BANK

Course Code/Name: 19GE5M03/ INTELLECTUAL PROPERTY RIGHTS

Sem/Year: V/III

Course Instructor/Coordinator Name: M. Yasmin, AP / CSBS

19GE5M03 - INTELLECTUAL PROPERTY RIGHTS
UNIT IV DIGITAL PRODUCT AND LAW
Digital innovation and developments as knowledge assets- IP laws, cyber law and digital content protection- unfair competition and IP laws-case studies

PART – A (2 Marks)

Q.No.	Question	Max. Marks	CO-L Level	PO-PI Code
1.	Getting patented is a painstaking process, complex as well costly to undergo. Therefore, being an option not possible forsmall scaled tech companies. Not only is costly, it does not secure that execution of the idea. In order to secure this, another form of protection is to be used can you mention it. Cubix is exposed to the most commonly voiced queries of clients that address issues related to protecting the source code and non-disclosure of the idea along with the proprietary algorithms to third parties.	02	CO 4-K3	1.6.1
2.	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 mention it. • 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.	02	CO 4-K2	1.2.1

	• 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 Aadharnumber is already in the wrong hands) • Do not fill personal data on the website that claim to offer benefits in return.			
3.	**Elucidate IPR Violation.Menion some.** **IPR violations :** These include software piracy, copyright infringement, trademarks violations, theft of computer source code, patent violations, etc.	02	CO 4- K3	2.5.1
4.	**Do you think cyber laws are needed? Justify your answer.** **Ans. : Yes,**The realm of cyberspace which is largely dependent upon the internet and use of technology, incidents of cybercrimes are reported to have increased. To protect one from cybercrime, there was a need for cyber laws and so the implementation of cyber laws in India began in the year 2000, with the IT Act as an introduction to Indian Cyber Law.	02	CO 4-K2	1.5.1
5.	**List some popular cybercrime that you know.** Identity- theft Cyber-terrorism Cyber-bullying Hacking	02	CO 4- K2	1.6.1
6.	**Mention some advantages of Cyber Laws.** **Ans. :** Advantages of cyber laws are; • Secured E-Commerce Infrastructure for online businesses. • Digitally sign your contracts/ papers. • Introduced new businesses for Certifying Authorities.	02	CO 4-K3	2.5.1

	• Proficient use of E-Forms as prescribed. • Secured websites with Digital Certificates. • Meticulous monitoring on the web traffics. • Electronic Transactions safeguarded. • Emails are a legal form of communication and are approved in the court of law.			
7.	**Mention some issues addressed by IT Act. Also, Mention its amendments.** The IT Act addresses the important issues of security, which are critical to the success of electronic transactions. The Internet Laws in India not only validates digital signatures but also provides for how authentication of the documents, which has been accepted and generated by using the digital signatures, can be done. the Information Technology Law was amended under ; the Indian Penal Code, the Indian Evidence Act, the Banker's Book Evidence Act, the Reserve Bank of India.	02	CO 4-K3	1.2.1
8.	**Do you think unfair competition diminishes reputation of any company or individual?** **Ans. : Yes,** All forms of deceptive trade practices can diminish the value associated with a commercial activity, product, service, or business value by confusing consumers, diverting sales,tarnishing reputations of goods, services, and commercial activities and can result in economic loss as well as injury. For example, a consumer may suffer injuries by mistakenly purchasing substandard products/services thinking they are related to another company or manufacturer.	02	CO 4 K3	1.6.1
9.	**List out the thrust areas of top digital solutions.** **Ans. :** The top digital solutions focus on the following 3 areas : Customer, Partner or Supplier Engagement Product and Service Innovation Internal Systems Processing, Reporting, or Access	02	CO 4- K2	2.5.1
10.	**If a student has developed an app. Can he can get the patent?** **Ans. P**atent protection for an app depends on which element of your app you wish to protect. If you want to protect a technical	02	CO 4-K3	1.6.1

	idea or feature relating to the app, patent protection is a potential option. You must be mindful however that your technical idea must meet all of the patentability requirements to obtain patent protection, and it may take years to get a patent.			

PART – B (13 Marks)

Q.No.	Question	Max. Marks	CO-K Level	PO-PI Code
1	The Competition Act, 2002 was enacted by the Parliament of India and governs Indian competition law. It replaced the archaic, The Monopolies and Restrictive Trade Practices Act, 1969. Under this legislation, the Competition Commission of India was established to prevent the activities that have an adverse effect on competition in India. This act extends to whole of India except the State of Jammu and Kashmir. Mention the Features of this Act and Objectives of CCI (Competition Commission of India) Objectives (3 marks) Types (3 marks) Features (7 marks)	13	CO4- K3	1.2.1
2	Enumerate about Cyber Law, Some laws create rules for how individuals and companies may use computers and the internet while some laws protect people from becoming the victims of crime through unscrupulous activities on the internet. Amongst mention major areas of cyber laws and protection measures. Cyber Law Definition (2 Marks) Areas (8 Marks) Protection Measures(3 marks)	13	CO4- K3	1.7.1
3	In the digital age the issue of privacy is an important subject where unauthorized data sharing, data integration, unethical data utilization and unauthorized public disclosure are the major areas	13	CO4- K4	2.8.4

	of concern. Discuss the issues based on IPR and Digital Rights, also List out the ways for protection of Digital / Intellectual Property. The rise in internet usage has resulted in rise of cybercrimes. The rise in cyber crimes resulted in an increased awareness of the importance of cyber security.So, Suggest the ways to use an internet security suite. Issues – 7 marks Ways -6 marks (Answers below)			
4	**Nasscom vs. Ajay Sood and Others Scenario:** In a landmark judgment in the case of National Association of Software and Service Companies vs. Ajay Sood & Others, delivered in March, '05, the Delhi High Court declared 'phishing' on the internet to be an illegal act, entailing an injunction and recovery of damages. A cybercrime case study has been conducted on the same. Elaborating on the concept of 'phishing', in order to lay down a precedent in India, the court stated that it is a form of internet fraud where a person pretends to be a legitimate association, such as a bank or an insurance company in order to extract personal data from a customer such as access codes, passwords, etc. Personal data so collected by misrepresenting the identity of the legitimate party is commonly used for the collecting party's advantage. The court also stated, by way of an example, that typical phishing scams involve persons who pretend to represent online banks and siphon cash from e-banking accounts after conning consumers into handing over confidential banking details. The Delhi HC stated that, even though there is no specific legislation in India to penalize phishing, it held phishing to be an illegal act, by defining it under Indian law as "a misrepresentation made in the course of trade, leading to confusion, as to the source and origin of the email causing immense harm, not only to the consumer, but even to the person whose name, identity or password is misused." The	13	CO3- K4	1.7.1

	court held the act of phishing as passing off and tarnishing the plaintiff's image. The plaintiff, in this case, was the National Association of Software and Service Companies (Nasscom), India's premier software association. The defendants were operating a placement agency involved in headhunting and recruitment. In order to obtain personal data, which they could use for purposes of headhunting, the defendants composed and sent emails to third parties, in the name of Nasscom The high court recognised the trademark rights of the plaintiff and passed an ex-parte ad interim injunction restraining the defendants from using the trade name or any other name deceptively similar to Nasscom. The court further restrained the defendants from holding themselves out as being associated with or a part of Nasscom. Question 1.Suggest some actions taken by you if you are a victim (3 Marks) 2. Mention the E-mail and IRC-related Crimes (10 Marks) (Answers below)			
5	**SONY.SAMBANDH.COM Case:** India saw its first cybercrime conviction in 2013. It all began after a complaint was filed by Sony India Private Ltd, which runs a website called www.sony-sambandh.com, targeting Non-Resident Indians. The website enables NRIs to send Sony products to their friends and relatives in India after they pay for it online.The company undertakes to deliver the products to the concerned recipients. In May 2002, according to the cybercrime case study, someone logged onto the website under the identity of Barbara Campa and ordered a Sony Colour Television set and a	13	CO4- K4	2.8.4

	cordless headphone. She gave her credit card number for payment and requested the products to be delivered to Arif Azim in Noida. The payment was duly cleared by the credit card agency, and the transaction was processed. After following the relevant procedures of due diligence and checking, the company delivered the items to Arif Azim.At the time of delivery, the company took digital photographs showing the delivery being accepted by Arif Azim. The transaction closed at that, but after one and a half months the credit card agency informed the company that this was an unauthorized transaction as the real owner had denied having made the purchase. **Question** **i)Do you think that we can legally file the case? If so under what section the company can file the case? (4 marks)** Yes, The company lodged a complaint about online cheating at the Central Bureau of Investigation which registered a case under Section 418, 419 and 420 of the Indian Penal Code. **ii)Exaggerate the situation what really happened? (4 marks)** The CBI recovered the colour television and the cordless headphone, in this one of a kind cyber fraud case. In this matter, the CBI had evidence to prove their case, and so the accused admitted hisguilt. The court convicted Arif Azim under Section 418, 419 and 420 of the Indian Penal Code - this being the first time that cybercrime has been convicted. The court, however, felt that as the accused was a young boy of 24 years and a first-time convict, a lenient view needed to be taken. The court, therefore, released the accused on probation for one year. The judgment is of immense significance for the entire nation. Besides being the first conviction in a			

	cybercrime matter, it has shown that the Indian Penal Code can be effectively applied to certain categories of cyber crimes which are not covered under the Information Technology Act 2000. Secondly, a judgment of this sort sends out a clear message to all that the law cannot be taken for a ride. **ii)BSNL, Unauthorized Access :** In a leading cybercrime case, the Joint Academic Network (JANET) was hacked by the accused, after which he denied access to the authorized users by changing passwords along with deleting and adding files. Making it look like he was authorized personnel, he made changes in the BSNL computer database in their internet users' accounts. When the CBI carried out investigations after registering a cybercrime case against the accused,they found that the broadband Internet was being used without any authorization. The accused used to hack into the server from various cities like Chennai and Bangalore, amongst others. This investigation was carried after the Press Information Bureau, Chennai, filed a complaint. In the verdict by the Additional Chief Metropolitan Magistrate, Egmore, Chennai, the accused from Bangalore would be sent to prison for a year and will have to pay a fine of ` 5,000 under Section 420 IPC. **iii)Do you think, this scenario comes under IT ACT? If yes mention the section. Suggest the ways how to avoid this kind of situations.(5 marks)** Yes,Section 66 of the IT Act. Own Answer			

COURSE INSTRUCTOR **H.O.D**

Qn No 1:

Salient Features of the Competition Act 2002

Anti Agreembents : Enterprises, persons or associations of enterprises or persons, including cartels, shall not enter into agreements in respect of production, supply, distribution, storage, acquisition or control of goods or provision of services, which cause or are likely to cause an "appreciable adverse impact" on competition in India. Such agreements would consequently be considered void. Agreements which would be considered to have an appreciable adverse impact would be those agreements which;

- Directly or indirectly determine sale or purchase prices,
- Limit or control production, supply, markets, technical development, investment or provision of services,
- Share the market or source of production or provision of services by allocation of inter alia geographical area of market, nature of goods or number of customers or any other similar way,
- Directly or indirectly result in bid rigging or collusive bidding.

Types of agreement : A 'horizontal agreement' is an agreement for co-operation between twoor more competing businesses operating at the same level in the market. A vertical agreement is an agreement between firms at different levels of the supply chain. For instance, a manufacturer of consumer electronics might have a vertical agreement with a retailer according to which the latter would promote their products in return for lower prices.

Abuse of dominant position : There shall be an abuse of dominant position if an enterprise imposes directly or indirectly unfair or discriminatory conditions in purchase or sale of goods or services or restricts production or technical development or create hindrance in entry of new operators to the prejudice of consumers. The provisions relating to abuse of dominant position require determination of dominance in the relevant market. Dominant position enables an enterprise to operate independently or effect competitors by action.

Combinations : The Act is designed to regulate the operation and activities of combinations, a term, which contemplates acquisition, mergers or amalgamations. Combination that exceeds the threshold limits specified in the Act in terms of assets or turnover, which causes or is likely to cause adverse impact on competition within the relevant market in India, can be scrutinized by the Commission.

<u>Objectives</u> of CCI are;

Anti-competitive agreements : This covers both the horizontal and vertical agreements. It states that four types of horizontal agreements between enterprises involved in the same industry would be applied. These agreements are those that :

Lead to price fixing; limit or control quantities; share or divide markets; and result in bid-rigging. It also identifies a number of vertical agreements subject to review under rule of reach test.

Abuse of dominance : The Act lists five categories of abuse :

- Imposing unfair/discriminatory conditions in purchase of sale of goods or services (including predatory pricing);

Combinations Regulation (Merger and Amalgamation) : The Act states that any combination

that exceeds the threshold limits in terms of value of assets or turnover can be scrutinized by the CCI to determine whether it will cause or is likely to cause an appreciable adverse effect on competition within the relevant market in India.

Enforcement : The CCI, the authority entrusted with the power to enforce the provisions of the Act, can enquire into possibly anti-competitive agreements or abuse of dominance either on its own initiative or on receipt of a complaint or information from any person, consumer, consumer's association, a trade association or on a reference by any statutory authority. It can issue 'cease and desist' orders and impose penalties. The CCI can also order the break-up of a dominant firm.

The new competition law in India, despite some concerns expressed in certain quarters, is much more consistent with the current anti-trust thinking than the outgoing MRTP Act. Although the success of the new Indian model will now turn on its implementation, India would appear to have taken a very substantial step towards the adoption of a modem competition policy.

Commission has the power to inquire into unfair agreements or abuse of dominant position or combinations taking place outside India but having adverse effect on competition in India, if any of the circumstances exists :

- An agreement has been executed outside India.
- Any contracting party resides outside India.
- Any enterprise abusing dominant position is outside India.
- A combination has been established outside India.
- A party to a combination is located abroad.
- Any other matter or practice or action arising out of such agreement or dominant position orcombination is outside India.

To deal with cross border issues, commission is empowered to enter into any memorandum of understanding or arrangement with any foreign agency of any foreign country with the prior approval of central Government.

- **Review of orders of Commission :** Any person aggrieved by an order of the Commission can apply to the Commission for review of its order within thirty days from the date of the order. Commission may entertain a review application after the expiry of thirty days, if it is satisfied that the applicant was prevented by sufficient cause from preferring the application in time. No order
- shall be modified or set aside without giving an opportunity of being heard to the person in whose favour the order is given and the Director General where he was a party to the proceedings.
- **Appeal :** Any person aggrieved by any decision or order of the Commission may file an appeal to the Supreme Court within sixty days from the date of communication of the decision or order of the Commission. No appeal shall lie against any decision or order of the Commission made with the consent of the parties.
- **Penalty :** If any person fails to comply with the orders or directions of the Commission shall be punishable with fine which may extend to 1 lakh for each day during which such non compliance occurs, subject to a maximum of 10 crore.

- If any person does not comply with the orders or directions issued, or fails to pay the fine imposed under this section, he shall be punishable with imprisonment for a term which will extend to three years, or with fine which may extend to 25 crores or with both.
- Section 44 provides that if any person, being a party to a combination makes a statement which is false in any material particular or knowing it to be false or omits to state any material particular knowing it to be material, such person shall be liable to a penalty which shall not be less than 50 lakhs but which may extend to 1 crore.

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 bothprosecute 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

Protection Measures

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.

Qn No:3

IPR and Digital Rights

In the digital age the issue of privacy is an important subject where unauthorized data sharing, data integration, unethical data utilization and unauthorized public disclosure are the major areas ofconcern. The major issues are to be considered as follows :

1. Is digitization to be considered as similar to reproduction, for example using Xerox machine ?
2. Is digitization a creative activity such as translation from one language to another ?
3. Can transmission of digitized documents through Internet be considered as commercial distribution or public communication similar to broadcasting ?
4. Can we consider database as a special collected work that should be protected by the copyright law ?
5. What can be considered as fair use in the Internet environment ?
6. What are the concerns of the library community ?
7. In the digital context if access restricted by the copyright owner, how could the public exercise fair use with those work ?

Whether all these activities will continue in the digital age ? If digitization is considered as reproduction work, it is quite clear that in digitization the initial work is merely changed into the digital form and the process of changing is accomplished by a machine, without any creativity. If it is considered as a translation from one language to another, the digitization is also a change from natural human language in to machine language. However in digitization, there is no creativity involved and it could be considered as a similar activity to reprography. The copyright protects only creative works. Simply transformation in to the digital form of an original document cannot be considered as creative work. The transmission of information on Internet can be considered similar to broadcasting; hence copyright law cannot be applied.

Ways for Protection of Digital / Intellectual Property

Digital Rights Management (DRM) technologies (also known as Electronic Rights Management Systems) ensure copyright through identifying and protecting the content, controllingaccess of the work, protecting the integrity of the work and ensuring payment for the access. DRM technologies prevent illegal users in accessing the content. Access is protected through user ID andpassword, licensing agreements. Another way to protect digital content is through Technical Protection Measures (TPM). These technologies allow publishing companies in securing and protecting content such as music, text and video from unauthorized use. If an author wishes to collect fee for use of his or her work, then DRM technology can be used. The TPM and DRM technologies are increasingly employed to sell and distribute content over the Internet.

Cryptography : Cryptography is the oldest mechanism employed to ensure security and privacy of information over networks. This involves scrambling (or encryption) of the information to render it unreadable or not understandable language, which only the legitimate user can unscramble (or decrypt). However cryptography protects the work during transmission or distribution only. After the work is decrypted, it does not provide any protection.

Digital Watermark Technology : A digital watermark is a digital signal or pattern inserted into a digital document. It is similar to the electronic on-screen logo used by TV channels. A unique identifier is used to identify the work. The message might contain information regarding ownership, sender, recipient etc or information about copyright permission. The system consists of a watermark generator, embedding and a watermark detector decoder. The legal user can remove these watermarks with a predetermined algorithm. The watermarking technology is extensively used in protecting multimedia works.

Digital Signature Technology : Digital signature includes identity of the sender and/or receiver date, time, any unique code etc. This information can be added to digital products. This digitally marks and binds a software product for transferring to a specified customer. Digitally signed fingerprints guarantee document authenticity and prevent illegal copying.

Electronic Marking : In this technique, the system automatically generates a unique mark that is tagged to each of the document copies. This technique is used to protect copyright as well as in electronic publishing where documents are printed, copied or faxed.

Qn No 4

Take appropriate actions if you have been a victim : There are few things that should be done as soon as you realize you have been hacked :

- File a formal complaint with the police and inform the other relevant authorities.
- Try regaining access to your compromised accounts by utilizing secondary contacts.
- Reset the password for other accounts and websites that were using the same password as theaccount that was compromised.
- Perform a factory reset and proper formatting of your devices that are affected (assuming youhave your data backed up already).
- Stay aware of the current data breaches and other incidents of the cyber world to prevent suchincidents from happening again and staying safe online.

E-mail and IRC related crimes

- **Email spoofing :** Email spoofing refers to email that appears to have been originated from one source when it was actually sent from another source.
- **Email spamming :** Email "spamming" refers to sending email to thousands and thousands of users , similar to a chain letter.
- **Sending malicious codes through email :** E-mails are used to send viruses, Trojans etc. through emails as an attachment or by sending a link of website which on visiting downloads malicious code.
- **Email bombing :** E-mail "bombing" is characterized by abusers repeatedly sending an identical email message to a particular address.
- Sending threatening emails
- **Defamatory emails**

- Email frauds
- **IRC related :** Three main ways to attack IRC are : "verbal>8218;?Ŧ#8220; attacks, cloneattacks and flood attacks.

Denial of service attacks : Flooding a computer resource with more requests than it can handle. This causes the resource to crash thereby denying access of service to authorized users. Examples include : attempts to "flood" a network, thereby preventing legitimate network traffic attempts to disrupt connections between two machines, thereby preventing access to a service attempts to prevent a particular individual from accessing a service attempts to disrupt service to a specific system or person.

Distributed DOS : A distributed denial of service (DoS) attack , is accomplished by using the Internet to break into computers and using them to attack a network. Hundreds or thousands of computer systems across the Internet can be turned into “zombies” and used to attack another system or website.

Types of DOS : There are three basic types of attack ;

- **Consumption** of scarce, limited, or non-renewable resources like NW bandwidth, RAM, CPU time. Even power, cool air or water can affect.
- ***Destruction or alteration of configuration information***
- Physical destruction or alteration of network components
- **Pornography :** The literal meaning of the term 'Pornography' is “describing or showing sexual acts in order to cause sexual excitement through books, films, etc.” This would include pornographic websites; pornographic material produced using computers and use of internet to download and transmit pornographic videos, pictures, photos, writings etc

- **Forgery :** Counterfeit currency notes, postage and revenue stamps, mark sheets etc. can be forged using sophisticated computers, printers and scanners.
- **IPR violations :** These include software piracy, copyright infringement, trademarks violations, theft of computer source code, patent violations, etc.

Cyber squatting : Domain names are also trademarks and protected by ICANN’s domain dispute resolution policy and also under trademark laws. Cyber squatters registers domain name identical to popular service provider’s domain so as to attract their users and get benefit from it.

Cyber terrorism : Targeted attacks on military installations, power plants, air traffic control, banks, trail traffic control, telecommunication networks are the most likely targets. Others like police, medical, fire and rescue systems etc. Cyber terrorism is an attractive option for modern terrorists for several reasons. Like; it is cheaper than traditional terrorist methods, cyber terrorism is more anonymous than traditional terrorist methods, the variety and number of targets are enormous, cyber terrorism can be conducted remotely, a feature that is especially appealing to terrorists, cyber terrorism has the potential to affect directly a larger number of people.

Banking/credit card related crimes : In the corporate world, Internet hackers are continually looking for opportunities to compromise a company’s security in order to gain access to confidential banking and financial information. Use of; stolen card information or fake credit/debit

cards are common. Bank employee can grab money using programs to deduce small amount of money from all customer accounts and adding it to own account also called as salami.

E-commerce/investment frauds : Sales and Investment frauds. An offering that uses false or fraudulent claims to solicit investments or loans, or that provides for the purchase, use or trade of forged or counterfeit securities.

Merchandise or services that were purchased or contracted by individuals online are never delivered.

The fraud attributable to the misrepresentation of a product advertised for sale through an Internet auction site or the non-delivery of products purchased through an Internet auction site.

Investors are enticed to invest in this fraudulent scheme by the promises of abnormally high profits.

- **Sale of illegal articles :** This would include trade of narcotics, weapons and wildlife etc., by posting information on websites, auction websites, and bulletin boards or simply by using email communication. Research shows that number of people employed in this criminal area. Daily peoples receiving so many emails with offer of banned or illegal products for sale.
- **Online gambling :** There are millions of websites hosted on servers abroad, offer online gambling. In fact, it is believed that many of these websites are actually fronts for money laundering.

- **Defamation :** Defamation can be understood as the intentional infringement of another person's right to his good name. Cyber defamation occurs when defamation takes place with the help of computers and / or the Internet. E.g. someone publishes defamatory matter about someone on a website or sends e-mails containing defamatory information to all of that person's friends. Information posted to a bulletin board can be accessed by anyone. This means that anyone can place. Cyber defamation is also called as Cyber smearing.

Cyber stacking : Cyber stalking involves following a person’s movements across the Internet by posting messages (sometimes threatening) on the bulletin boards frequented by the victim, entering the chat-rooms frequented by the victim, constantly bombarding the victim with emails etc. In general, the harasser intends to cause emotional distress and has no legitimate purpose to hiscommunications.

Pedophiles : Also there are persons who intentionally prey upon children. Especially with a teen they will let the teen know that fully understand the feelings towards adult and in particular teen parents. They earn teens trust and gradually seduce them into sexual or indecent acts. Pedophiles lure the children by distributing pornographic material, and then they try to meet them for sex or to take their nude photographs including their engagement in sexual positions.

Identity theft : Identity theft is the fastest growing crime in countries like America. Identity theft occurs when someone appropriates another's personal information without their knowledge to commit theft or fraud. Identity theft is a vehicle for perpetrating other types of fraud schemes.

Data diddling : Data diddling involves changing data prior or during input into a computer. In other words, information is changed from the way it should be entered by a person typing in the

data, a virus that changes data, the programmer of the database or application, or anyone else involved in the process of having information stored in a computer file. It also includes automatic changing the financial information for some time before processing and then restoring original information.

Theft of internet hours : Unauthorized use of Internet hours paid for by another person. By gaining access to an organisation's telephone switchboard (PBX) individuals or criminal organizations can obtain access to dial-in/dial-out circuits and then make their own calls or sell call time to third parties. Additional forms of service theft include capturing 'calling card' details and on-selling calls charged to the calling card account, and counterfeiting or illicit reprogramming of stored value telephone cards.

- **Theft of computer system (Hardware) :** This type of offence involves the theft of a computer, some part(s) of a computer or a peripheral attached to the computer.
- **Physically damaging a computer system :** Physically damaging a computer or its peripherals either by shock, fire or excess electric supply etc.

- Breach of privacy and confidentiality

Privacy : Privacy refers to the right of an individual/s to determine when, how and to what extent his or her personal data will be shared with others. Breach of privacy means unauthorized use or distribution or disclosure of personal information like medical records, sexual preferences, financial status etc.

Confidentiality : It means non disclosure of information to unauthorized or unwanted persons. In addition to personal information some other type of information which useful for business and leakage of such information to other persons may cause damage to business or person, such information should be protected.

Generally for protecting secrecy of such information, parties while sharing information forms an agreement about the procedure of handling of information and to not to disclose such information to third parties or use it in such a way that it will be disclosed to third parties.

Many times party or their employees leak such valuable information for monitory gains and causes breach of contract of confidentiality.

Special techniques such as social engineering are commonly used to obtain confidential information.