Prohibited actions on cyber

Pornography

- **What is Pornography?**

Cyber Pornography can be defined as pornographic material designed, published or distributed using cyber space as a medium. In India, viewing digital pornography is not a crime, but creating and distributing such material is. It is legal in most other countries. However, child pornography is illegal in all forms and has been banned universally.

- **What are the threats?**

In order to increase traffic, some websites resort to publishing free pornographic material. In addition, fraudsters have set up many malicious websites, whose sole purpose is to infect machines, which attract and lure people with offers like free celebrity pornography. Most of the material available for free download acts as a carrier of malware. Although viewing porn online is legal, it can also become an addiction due to the vast amount of free available material on the internet.

- **What are the Risks?**

Malware can steal crucial information from a system or a network.

Malware can damage systems leading to network failures.

Can be used for cyber defacement, defamation attacks leading to reputation loss.

Addiction to internet porn can ruin your social relationship in real life and cause embarrassment in work life.

Intellectual property rights

- Intellectual property rights are the legal rights that cover the privileges given to individuals who are the owners and inventors of a work, and have created something with their intellectual creativity. Individuals related to areas such as literature, music, invention, etc., can be granted such rights, which can then be used in the business practices by them.

Intellectual Property Rights can be further classified into the following categories –

- Copyright
- Patent
- Trademarks
- Trade Secrets,
- Designs etc.

Advantages of Intellectual Property Rights

- Provides exclusive rights to the creators or inventors.
- Encourages individuals to distribute and share information and data instead of keeping it confidential.
- Provides legal defence and offers the creators the incentive of their work.
- Helps in social and financial development.

Threats

- Every new invention in the field of technology experiences a variety of threats. Internet is one such threat, which has captured the physical marketplace and have converted it into a virtual marketplace.
- To safeguard the business interest, it is vital to create an effective property management and protection mechanism keeping in mind the considerable amount of business and commerce taking place in the Cyber Space.

Measures

- Creating a Secure Cyber Ecosystem
- Creating an Assurance Framework
- Encouraging Open Standards
- Strengthening the Regulatory Framework
- Creating Mechanisms for IT Security
- Securing E-governance Services
- Protecting Critical Information Infrastructure

IPR Violations

Software piracy

- **Software piracy** is defined as illegally copying **software** that does not belong to you in a manner that violates the copyright. A example of **software piracy** is when you download a copy of Microsoft Word from a file-sharing website without paying for it.
- There Are Five Main Types of Software Piracy
- **Counterfeiting**
  This type of piracy is the illegal duplication, distribution and/or sale of copyrighted material with the intent of imitating the copyrighted product. In the case of packaged software, it is common to find counterfeit copies of the compact discs incorporating the software programs, as well as related packaging, manuals, license agreements, labels, registration cards and security features.
- **Internet Piracy**
  This occurs when software is downloaded from the Internet. The same purchasing rules apply to online software purchases as for those bought in compact disc format. Common Internet piracy techniques are:
- Websites that make software available for free download or in exchange for others
- Internet **auction sites** that offer counterfeit or out-of-channel software
- Peer-to-peer networks that enable unauthorized transfer of copyrighted programs
- **End User Piracy**
  This occurs when an individual reproduces copies of software without authorization. These include:
- Using one licensed copy to install a program on multiple computers
- Copying discs for installation or distribution
- Taking advantage of upgrade offers without having a legal copy of the version to be upgraded
- Acquiring academic or other restricted or non-retail software without a proper license
- Swapping discs in or outside the workplace
- **Client-Server Overuse**
  This type of piracy occurs when too many users on a network are using a central copy of a program at the same time. If you have a local-area network and install programs on the server for several people to use, you have to be sure your license entitles you to do so. If you have more users than allowed by the license, that's "overuse."
- **Hard-Disk Loading**
  This occurs when a business sells new computers with illegal copies of software loaded onto the hard disks to make the purchase of the machines more attractive.

Copyright infringement

- Copyright infringement is the use or production of copyright-protected material without the permission of the copyright holder. Copyright infringement means that the rights afforded to the copyright holder, such as the exclusive use of a work for a set period of time, are being breached by a third party. Music and movies are two of the most well-known forms of entertainment that suffer from significant amounts of copyright infringement.

Trademark violation

- The definition of Infringement of a registered trademark is given in Indian Trademarks Act of 1999, section 29 whereby, a registered trademark is said to be infringed by any person, who not being the registered proprietor of the Mark or being a person authorized by the owner for its use (registered user), uses in the course of trade, a mark which is identical with, or deceptively similar to the mark in relation to goods and services in respect of which the trademark is registered.

Patent violations

- **Patent infringement** is the commission of a prohibited act with respect to a patented invention without permission from the patent holder. Permission may typically be granted in the form of a license. The definition of patent infringement may vary by jurisdiction, but it typically includes using or selling the patented invention. In many countries, a use is required to be *commercial* (or to have a *commercial* purpose) to constitute patent infringement.[*citation needed*]
- The scope of the patented invention or the extent of protection[1] is defined in the claims of the granted patent. In other words, the terms of the claims inform the public of what is not allowed without the permission of the patent holder.
- Patents are territorial, and infringement is only possible in a country where a patent is in force. For example, if a patent is granted in the United States, then anyone in the United States is prohibited from making, using, selling or importing the patented item, while people in other countries may be free to exploit the patented invention in their country. The scope of protection may vary from country to country, because the patent is examined -or in some countries not substantively examined- by the patent office in each country or region and may be subject to different patentability requirements.

Cybersquatting

- Cybersquatting is registering, selling or using a domain name with the intent of profiting from the goodwill of someone else's trademark. It generally refers to the practice of buying up domain names that use the names of existing businesses with the intent to sell the names for a profit to those businesses.
- For example, Dell filed a lawsuit in 2007 against another party that had registered the URL "DellFinacncialServices.com" and 1,100 others, alleging cybersquatting. In that case, the defendants had registered misspelled confusingly similar domains to those owned by Dell with the intention of capturing the traffic from people mistyping "DellFinancialServices.com."

Online Defamation / Cyber Smearing

- Defamation is injury to the reputation of a person. Cyber defamation occurs when defamation takes place with the help of computers or the Internet.
- **The three essentials of defamation are:**
- The statement must be false and defamatory,
- The said statement must refer to the victim, and
- The statement must be published.
- A person's reputation is his or her property and sometimes even more valuable than physical property.
- Cyber criminals may also disclose victims' personal data (e.g. real name, address, or workplace/ schools) on various immoral websites.
  Cases of piggy-backing on victim's identity are now common. This could be used to publish objectionable material in their name that defames or ridicules a person.
- **Digital impersonation is one of the most dangerous kinds of online reputation problems. It happens when someone else assumes your identity and communicates using your real name, photograph or avatar.**
- Impersonator could either hack into your real accounts; or just create fake profiles or comments purporting to be "you." The motivation behind the act may be revenge, sadism, extortion, or playing some kind of twisted prank. The damage to reputation caused by impersonating someone online can be substantial and hard to cope with.

Credit card related crimes

- Credit card fraud is a form of identity theft in which an individual uses someone else's credit card information to charge purchases, or to withdraw funds from the account. Credit card fraud also includes the fraudulent use of a debit card, and may be accomplished by the theft of the actual card, or by illegally obtaining the cardholder's account and personal information, including the card number, the card's security number, and the cardholder's name and address.
- **Definition of Credit Card Fraud**
- The unauthorized use of an individual's credit card or card information to make purchases, or to remove funds from the cardholder's account.

- If you're a credit card holder, chances are pretty high that you'll become a victim of credit card theft or fraud at some point in your life, especially as e-commerce and other online payment activities become increasingly common. Theft and fraud can happen on a smaller scale, too: Your wallet can be stolen, or a family member can use your Social Security number to open a new card in your name.
- **How severely is credit card theft and fraud punished?**
- Different states prosecute fraud differently. In addition to the identity theft itself, criminals can be punished under federal law for using devices that facilitate fraudulent activity, such as skimmers or other counterfeit access devices. Minor offenses can result in fines, jail time, or both, but felony-level credit card theft and fraud can lead to prison.
- **How to protect yourself from credit card fraud**
- **Follow good safety practices**
- **Consider freezing your credit reports**
- **Contact authorities as soon as you notice fraudulent activity.**

Thank You..!!