4 CYBER LAW

Let us Learn

- Introduction to Cyber Law.
- Ethics and Morals.
- Cyber crime and its examples.
- Cyber Safety and Security
- IT Act 2000.
- Case Studies

4.1 Introduction

Today we use computers for storing confidential data from various sectors such as banking, finance, health, personal property etc. We also use internet for transactions of information related to these sectors. But in many situations, the confidential data may be illegally used, and corrupted by unauthorised users. The increase in Internet traffic has led to a higher proportion of legal issues worldwide. So it is very necessary to protect such data from Cyber criminals. Cyber cases related to interference and investigation are increasing at an alarming rate. To control such crimes, it is necessary to follow ethics in field of computer. Cyberlaw is being amended quite regularly.

Introduction to Cyberlaw :

Cyberlaw is the area of law that deals with the Internet's relationship to technological and electronic elements, including computers, software, hardware and information systems (IS).

Cyberlaw is the part of the overall legal system that deals with the Internet, cyberspace, and their respective legal issues. Cyber law covers a fairly broad area, encompassing several subtopics including freedom of expression, access to and usage of the Internet, and online privacy.

Advantages of Cyber Law :

The IT Act 2000 attempts to change outdated laws and provides ways to deal with cybercrimes. We need such laws so that.

- People can perform transactions over the Internet through credit cards without fear of misuse.
- The IT Act offers the much-needed legal framework so that information is not denied legal effect, validity or enforceability, solely on the ground that it is in the form of electronic records.
- In view of the growth in transactions and communications carried out through electronic records, the Act seeks to empower government departments to accept filing, creating and retention of official documents in the digital format.
- The IT Act has also proposed a legal framework for the authentication and origin of electronic records/ communications through digital signature.

Do it yourself

- Search Cyber crime related Laws & punishment for it.

4.2 Ethics and Morals

- **Ethics :** Also called moral philosophy is the discipline concerned with what is morally good and bad, right or wrong.
- **Morals :** The standards of behaviour; principles of right and wrong behaviour. Thus morals are dictated by society, culture or religion while ethics are chosen by the person himself which governs his life. This chapter introduces the do's and dont's of cyber world.

4.3 Cyber Crime

Computer Crime is alternatively referred to as cybercrime, e-crime, (electronic crime) or hi-tech crime. Computer crime is an act performed by a knowledgeable computer user, sometimes referred to as a **hacker** who illegally browses or steals a company's or individual's private information. In some cases, this person or group of individuals may be malicious and destroy or otherwise corrupt the computer or data files.

Cyber crimes can involve criminal activities that are traditional in nature, such as theft, fraud, forgery, defamation and mischief, all of which are subject to the Indian Penal Code.

Some Examples of cyber crime :

Below is a list of the different types of computer crimes -

- **Software Piracy :** Software piracy is nothing but copyright violation of software created originally by an individual or an institution. It includes stealing of codes/ programs and other information illegally and creating the imitated copy by unauthorized means and utilizing this data either for own benefit or for profit making.

  Example : When you download a copy of a licensed software. For example downloading games from a file sharing website without paying for it, it is a software piracy.

- **Unauthorized access :** Gaining access without the users' permission is known as unauthorized access. Authorization means granting access rights to resources, which is related to information security computer security and to access control in particular sector. This is typically possible when the particular software/service is purchased through legal and formal procedure. Attempting to get information (like emails, bank account, intellectual or any other personal and confidential information) from unauthorized person is known as accessing the machine illegally. Examples of unauthorized access are :
  - Hacking financial / bank account related information.
  - Stealing organizational / intellectual information.
  - Illegal monitoring of information owned by other users.
  - Illegal use/break of login and password of other users.

- Causing intentional irritation to other users by means of damaging software and important information.

- **Copyright violation :** A copyright is a legal right that gives the creator of a literary, artistic, musical, or other creative work the sole right to publish and sell that work. Copyright owners have the right to control the reproduction of their work, including the right to receive the royalty payment for that reproduction. © is copyright symbol.
- **Cracking :** Activity such as decipher codes or passwords and breaking security systems for illegal reasons is called cracking. The cracker will use a program or script known as a crack that has been written specifically to do what they're hoping to achieve.
- **Cyberbully or Cyberstalking :** Cyberstalking is a criminal practice where an individual uses the Internet to systematically harass or threaten someone. This crime can be perpetrated through email, social media, chat rooms, instant messaging client and any other online medium.
- **Phishing :** This a technique of extracting confidential information such as credit card numbers and username password combos by pretending as a legal enterprise. Phishing is typically carried out by email spoofing.
- **Plagarism :** Plagarism is presenting someone else's work or idea as your own without their consent. The widespread use of computers and the advent of the internent has made it easier to palagiarize the work of others. For example plagarism is found in document such as essay, reports etc.
- **Hacking :** Hacking refers to unauthorised intrusion into a computer or a network. Hacker is a person intensely interested in the deep and hidden or concealed working of any computer operating system and programming language. They might discover loopholes within systems and reasons for such loopholes.

Do it yourself

- List out Cyber Crime which you find in your surrounding.

Protecting Ourselves From Cyber Crime :

4.4 Cyber Safety and Security

Cyber safety is the safe and responsible use of information and communication technology. It is not just about keeping information safe and secure, but also about being responsible with that information, being respectful of other people online, and practising good 'netiquette' (internet etiquette). In recent years, all systems are exposed to Internet; hence there is increased challenge in maintaining and protecting them from the attackers.

Any organisation plays a key role in promoting internet safety. They are primarily responsible for keeping

systems/ computers/ network devices secure and functional.

The overall sequence from identifying threats to protecting and recovering from Cyber attacks and threats for organisations.

1) Identify threats and risk :

- The system (Computer) operates slowly with more response time.
- If the system crashes suddenly and unable to download updates.
- Appearance of new , unfamiliar icons or messages on desktop.

2) Protection of data :

- Protect the network with firewall.
- Create different logins and strong passwords for different users.
- Use only verified open source or licensed software and operating systems.
- Prohibit use of personal devices on the network, such as personal USBs or hard drives.
- Protect your Wi-Fi Connection with secure password, WEP encryption, etc. Encrypt the network traffic.

3) Recovery from cyber attack :

- After the cyber attack data should be cleaned, recovered and restored, as much as possible.
- Investigation should be carried out with support from an professional expert.
- Measures should be taken to avoid re-occurrence.

4) Educate your stakeholders(students, staff etc) :

- Introduce courses / lessons / activities for students and teachers on major components of cyber security and safety.

Do's and Don'ts for students in cyber world.

Do's :

1. Adhere to copyright restrictions when downloading material from the Internet, including software, games, movies, or music.
2. Report online bullying immediately to the teacher and parents/ or some one whom you trust.
3. Use a strong and unique password with combinations of numbers, uppercase and lowercase letter and special characters for each account(s) and change your password frequently.
4. Obtain software from trusted sources. Always scan files before opening them.
5. Check to see if the web address begins with https:// whenever you sign in online.
6. Connect only with known individuals.
7. Think twice before you post/like/ share something related to sensitive topics like politics, religion etc.
8. Report to the service provider immediately if the account is hacked. If possible deactivate your account.

Don’ts :

1. Don't share your personal information: real name, date of birth, phone number etc. unnecessarily.
2. Don't send your pictures to unknown persons or share them on social media.
3. Don't open emails and attachments from strangers.
4. Don't respond to any suspicious email, instant message or web page asking for personal information.
5. Don't share your password/OTP with anyone.
6. Don't save your username and password on the browser.
7. Don't steal other's information.
8. Don't access or use files without the permission of the owner.
9. Don't copy software which has copyright without the author's permission.
10. Don't bully others online by teasing, threatening, using rude or offensive language, making derogatory or hateful comments.
11. Don't meet unknown (even if they are known only through online interaction) people alone; always inform an adult or a friend.
12. Don't open or download any attachments from an unknown source as they may be harmful.

Security Procedures

- **Encryption :** It is a method of converting the original message into random text, which should be complex to understand and difficult for a hacker to decode. The idea is to ensure security and safety of data and its transmission.
- **SSL (Secure Socket Layer) :** It is the most consistent security model. Through the SSL, transmission of data is encrypted, client-server information is authenticated and also message integrity for TCP/IP connections secured.
- **Firewall :** Firewall refers to network security (Hardware and Software) system which blocks certain type of information, forming a barrier between a trusted and untrusted network. It attempts to block the spread of computer attacks.

Parental guidance :

A lot of cybercrimes revolve around unsuspecting teenagers and school children. Parents play a vital role in ensuring that their children are safe on the internet and not vulnerable to hackers and identity theft. To start with, treat confidential information as confidential. Never reveal sensitive data on the internet. Tell children not to give out personal information like address or telephone number or Facebook password to friends. Ensure, children don’t do that as vital information should be kept secret.

Do it yourself

- List out Security techniques to protect your computer data.

4.5 IT Act of India 2000

In May 2000, both the houses of the Indian Parliament passed the Information Technology Bill. The Bill received the assent of the President in August 2000 and came to be known as the Information Technology Act, 2000. Cyber laws are contained in the IT Act, 2000. IT act 2000 is an Act to provide legal recognition for transaction carried out by means of electronic data interchange and other means of electronic communication.

This Act aims to provide the legal infrastructure for e-commerce in India. The cyber laws have a major impact for e-businesses and the new economy in India. So, it is important to understand what are the various perspectives of the IT Act, 2000 and what it offers.

The Information Technology Act, 2000 also aims to provide for the legal framework so that legal goodness is accorded to all electronic records and other activities carried out by electronic means. The Act states that unless otherwise agreed, an acceptance of contract may be expressed by electronic means of communication and the same shall have legal validity and enforceability.

Salient Features of I.T. Act :

The salient features of the I.T Act are as follows :

- Digital signature has been replaced with electronic signature to make it a more technology neutral act.
- It elaborates on offenses, penalties, and breaches.
- It outlines the Justice Dispensation Systems for cyber-crimes.
- It defines in a new section that cyber café is any facility from where the access to the internet is offered by any person in the ordinary course of business to the members of the public.
- It provides for the constitution of the Cyber Regulations Advisory Committee.
- The IT Act 2000 was amended in 2008 and 2011 and it includes rules for cyber cafe, cyber security, delivery of services by service provider, Audit of electronic document etc.

Do it yourself

- Find out new amendments in IT Act 2000.

Case study 1

Mr. A checked his account .His account displayed deduction of Rs 30,000. Investigation revealed the money had been transferred to Mr, B's account. He was informed that he has been a victim of cybercrime. He had given his password and name online by replying to an email sent by the hackers.

The hackers then logged into Mr. A's account and put in their mobile number instead of his. So that,when they did make the transfer,the message alert of the transfer would go to their mobile and not his. Phishing normally begins by," you

getting an mail-let's say from the bank-saying that some one is trying to hack into you account so you need to re-give your password. So, you click on the link. That website is a fake or the spoofed website you don't realize that your user name and password has gone to the phisher.

Answer the following based on the case study

1) What type of cybercrime does the case study refer to ?

2) What does the term hacker mean ?

3) How did Mr. A become a victim of Cybercrime ?

4) What precautions should been taken in order to avoid this type of fraud ?

Case study 2

Source Code Theft Case :

Indian IT company gave bug fixing project for their source code by a US company. One of the employees secretly took away the source code on two CDs Tried to sell the source code to other US companies and demanded a price of US $ 200,000 he also received advance payment of US $20,000 by wire transfer. Case registered against him and got arrested.

Case study 3

Fake Call Frauds

Several instances have occurred wherein people receive phone calls that appear to be from their bank. The caller usually pretends to be a bank presentative or someone from the bank's technical team. In most cases, the caller sounds professional and provides a convincing reason for calling the customer. After giving a false sense of security, the caller then tricks the victim into giving away their personal and confidential data such as :

- One-Time-Password (OTP), Credit/ debit card number, The card's CVV number, Expiry date, Secure password, ATM pin, Internet Banking login ID and password and other personal information

With all such crucial information at hand, the fraudster can easily carry out illegal financial transactions using the victim's name.

Students are encouraged to get more recent local case studies and discuss in the class. **(case study 2 and case study 3 are for study purpose)**

Do it yourself

- Search some more cases of cyber crime investigated.

Note : *Digital Signatures were used for authentication and security of documents. But now a days digital signatures are replaced by e-signature which is based on AADHAAR to check individuals authentications.*

Do it yourself

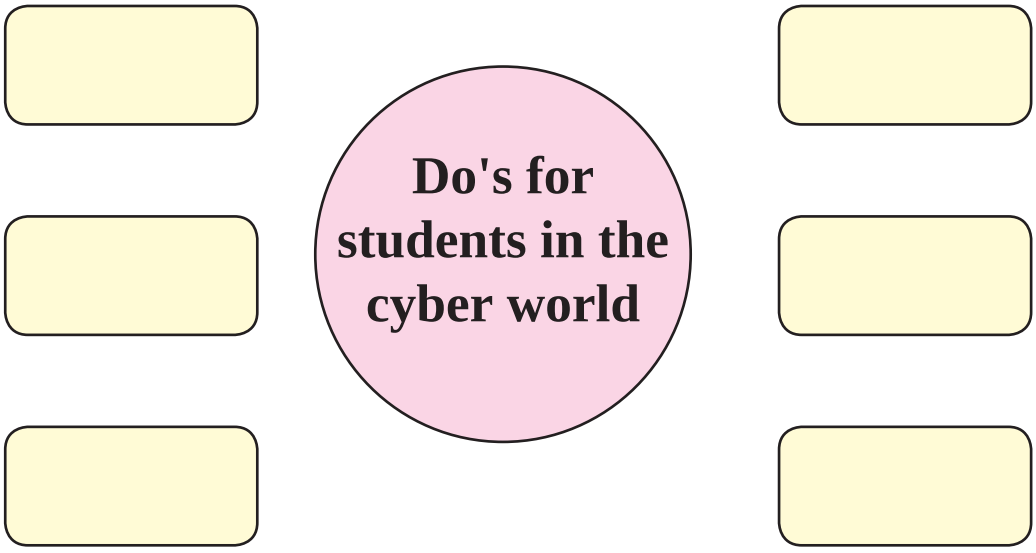
Find out atleast Three more security procedures adopted by during electronic transactions by companies.

Find out new amendments in IT Act 2008.

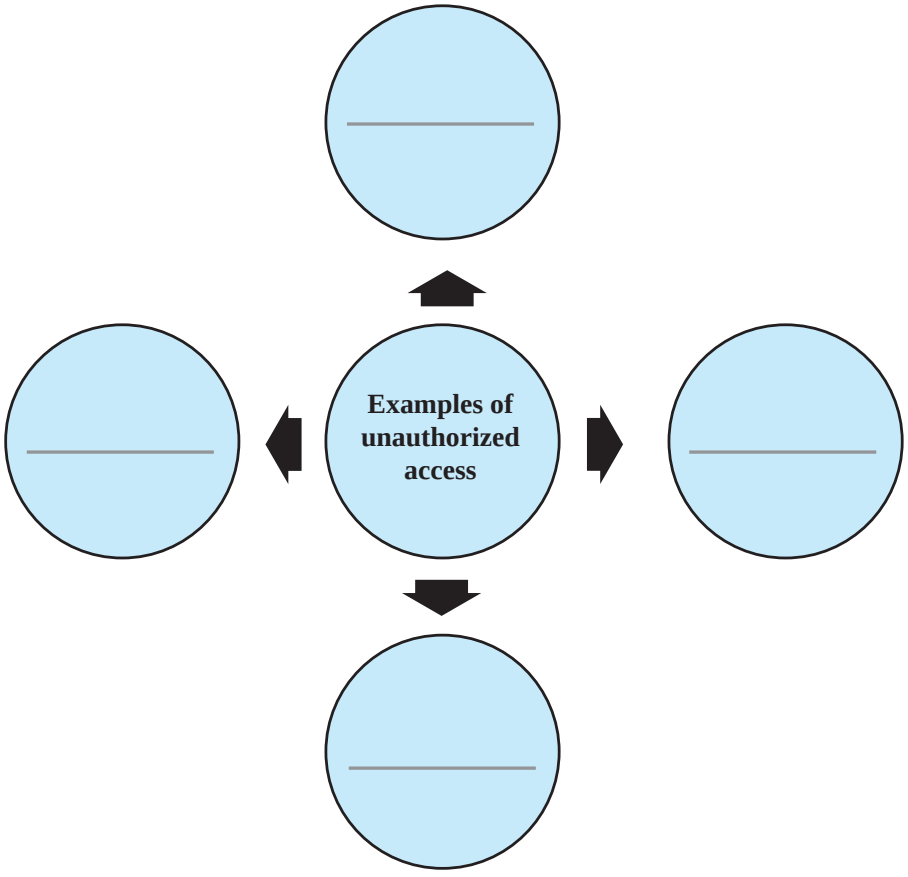
Summary

- The increase in internet traffic has led higher level of interference and investigation at alarming rate.
- To control cyber crimes it is necessary to give moral and ethical education to computer user at the same time it is necessary to aware users about cyber laws for such crimes.
- Cyber law is the area of law that deals with the internet, cyberspace and their respective legal issues.
- Cyber crime can involve criminal activity such as unauthorised access to others computer, copyright violation, cracking code and websites, creating malware, software piracy etc.
- Every computer user must follow the Do's and Don'ts to live in this cyber world.
- Every one should know the IT Act 2000 and its features to safeguard themselves from cyber crime.

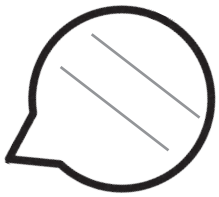
Q 1. Complete the following web.



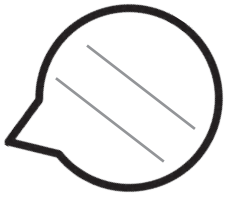
Q 2. Complete the following chart.



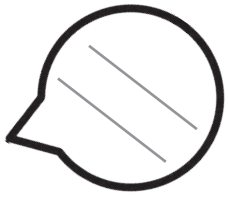
Q3. Fill following boxes with appropriate cyber crime name



1) Copyright violation of software created originally by an individual.



2) Gaining access without the user's permission



3) Extracting confidential information by email.

Q 4. Read the following and answer the question.

Rahul lost his pen drive in his college computer lab. His classmate Madhav finds it .He carries it home to return it to him the next day. When Madhav opens it he finds his favourite game. He thinks of making a duplicate copy of the game software.

I) Does Madhav think ethically ?

II) What do you think should Madhav do ?

III) If he makes a duplicate copy then which cyber crime will he commit ?

Q 5. Answer in brief

1) What care should be taken by the user while doing online activities ?

2) Define the terms (1) Ethics (2) Moral

3) Explain three examples related to unauthorized access?

4) Explain software piracy and Hacking

Q.6. State true or false

1) Firewall is used to encrypt transmission of data.

2) The standards of behaviour; principle of right or wrong is referred as moral.

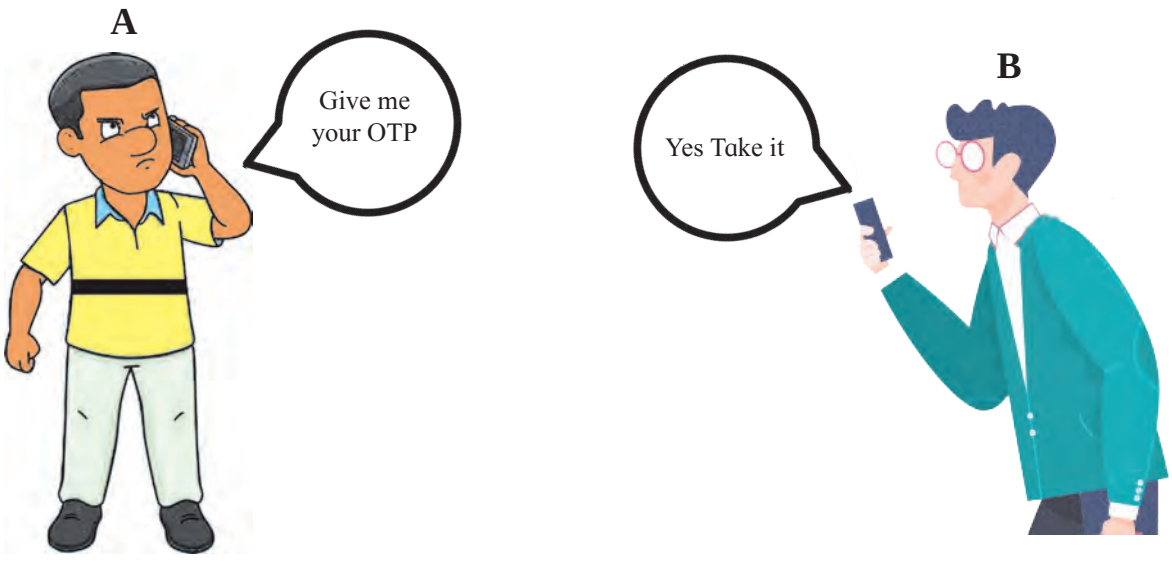
3) Hacking bank account related information is an example of software piracy.

4) Phishing is representing some one else's work as own without permission.

Q.7 Match the following.

(A)	(B)
(1) Copying a game file	(a) Firewall
(2) Law related to internet	(b) Cyber threat
(3) Network security	(c) Software piracy
(4) System crashes suddenly	(d) Cyber Law

Q 8. Observe the following picture and give your opinion about it by responding to the following questions.



1) Is '**B**'s response correct or not ?

2) What will be the consequences of '**B**'s reply ?

3) Which type of cyber crime does the picture depict ?


Want to Design a Web Page
WEB DESIGN
Hello !!!
I'm Jr. Accountant
BANK
Wanna edit
my video & add music?
Be Different
SKILL ORIENTED
PRACTICALS
(SOP)
Be Creative
Be Innovative
Type Fast