Computer Ethics and Cyber Security

Learning Objectives

After learning this chapter, the students will be able to

- To know about cyber-crimes.
- To understand the guidelines and need for ethics in cyber-world.
- To understand issues related to cyber-crimes.
- To know the functionality of firewalls and proxy servers.
- To learn about encryption and decryption.
- To gain knowledge on IT Act.

17.1 INTRODUCTION

Internet is a communication media which is easily accessible and open to all. Information Technology is widespread through computers, mobile phones and internet. There is a lot of scope and possibility for misuse of Information Technology.

Computer systems in general are vulnerable.Special care must be taken explicitly in order to ensure that the valuable data do not get into wrong hands. Hence, the data need to be protected.

A cyber-crime is a crime which involves computer and network.This is becoming a growing threat to society .

ETHICS

Ethics is a set of moral principles that govern the behavior of an individual in a society, and Computer ethics is set of moral principles that regulate the use of computers by users.

GUIDELINES OF ETHICS

Generally, the following guidelines should be observed by computer users:

1. **Honesty:** Users should be truthful while using the internet.
2. **Confidentiality:** Users should not share any important information with unauthorized people.
3. **Respect:** Each user should respect the privacy of other users.
4. **Responsibility:** Each user should take ownership and responsibility for their actions

Ethics is a set of moral principles that govern the behavior of an individual in a society, and Computer ethics is set of moral principles that regulate the use of computers by users.

17.2 ETHICAL ISSUES

An Ethical issue is a problem or issue that requires a person or organization to choose between alternatives that must be evaluated as right (ethical) or wrong (unethical). These issues must be addressed and resolved to have a positive influence in society.

Some of the common ethical issues are listed below:

- Cyber crime
- Software Piracy
- Hacking
- Use of computers to commit fraud

- Sabotage in the form of viruses
- Making false claims using computers

CYBER CRIME

Cybercrime is an intellectual, white-collar crime. Those who commit such crimes generally manipulate the computer system in an intelligent manner.

For example – illegal money transfer via internet.

Examples of some Computer crimes and their functions are listed below in **Table 17.1:**

Table 17.1 Computer Crime

Crime	Function
Malware	Malicious programs that can perform a variety of functions including monitoring user's computer activity without their permission.
Harvesting	A person or program collects login and password information from a legitimate user to illegally gain acces s to others' account(s).
Spam	Distribute unwanted e-mail to a large number ofinternet users.

SOFTWARE PIRACY

Software Piracy is "unauthorized copying of software". **Figure 17.2** shows a diagrammatical representation of software piracy.

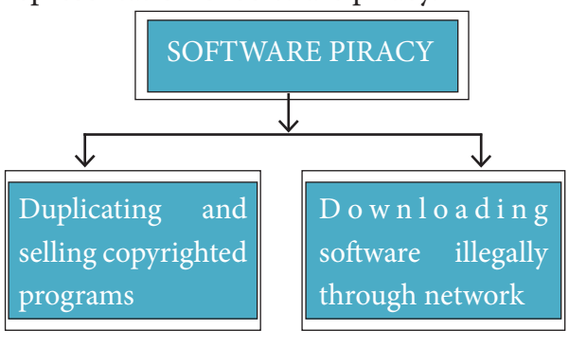

Figure 17.2- Diagrammatic representation of Software piracy

An entirely different approach to software piracy is called **Shareware**. Shareware publishers encourage users to give copies of programs to friends and colleagues but ask everyone who uses that program regularly to pay a registration fee to the program's author directly. Commercial programs that are made available to the public illegally are often called **Warez**.

HACKING

Hacking is intruding into a computer system to steal personal data without the owner's permission or knowledge (like to steal a password). It is also gaining unauthorized access to a computer system, and altering its contents. It may be done in pursuit of a criminal activity or it may be a hobby. Hacking may be harmless if the hacker is only enjoying the challenge of breaking systems' defenses, but such ethical hacking should be practiced only as controlled experiments. **Figure 17.3** shows a diagrammatic representation of Hacking.

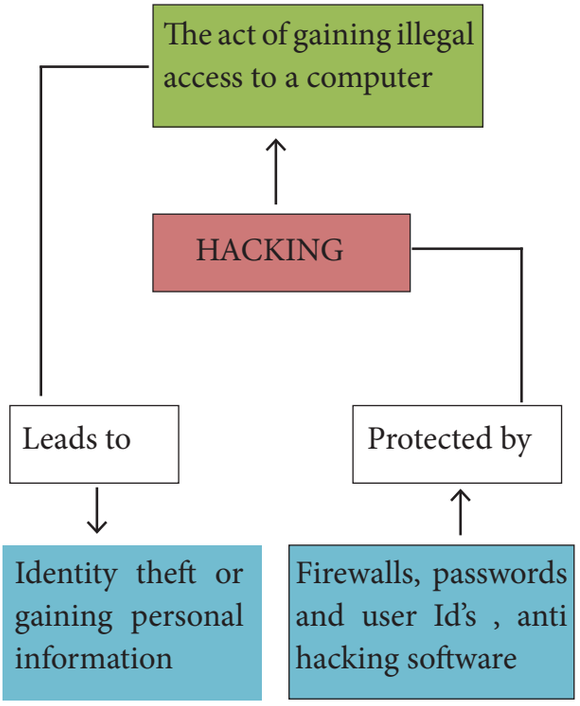

Figure 17.3 Diagramatic representation of Hacking

To prevent unauthorized access, Firewalls, **Intrusion Detection Systems** (IDS), Virus and Content Scanners, Patches and Hot fixes are used.

CRACKING

Cracking is where someone edits a program source so that the code can be exploited or modified. A cracker (also called a black hat or dark side hacker) is a malicious or criminal hacker. "Cracking" means trying to get into computer systems in order to steal, corrupt, or illegitimately view data.

A cracker is someone who breaks into someone else's computer system, often on a network, bypassing passwords or licenses in computer programs.

They may send official e-mail requesting some sensitive information. It may look like a legitimate e-mail from bank or other official institution.

17.3 Cyber Security and Threats

Cyber attacks are launched primarily for causing significant damage to a computer system or for stealing important information from an individual or from an organization.Cyber security is a collection of various technologies, processes and measures that reduces the risk of cyber attacks and protects organizations and individuals from computer based threats.

TYPES OF CYBER ATTACKS

Malware is a type of software designed through which the criminals gain illegal access to software and cause damage. Various types of cyber-attacks and their functions are given in**Table 17.2.**

Table 17.2 – Cyber Attacks and Functions

S.No.	Cyber Attack	Function
1.	Virus	A virus is a small piece of computer code that can repeat itself and spreads from one computer to another by attaching itself to another computer file. One of the most common virus is **Trojan**. A Trojan virus is a program that appears to perform one function (for example, virus removal) but actually performs malicious activity when executed.
2.	Worms	Worms are self- repeating and do not require a computer program to attach themselves. Worms continually look for vulnerabilities and report back to the author of the worm when weaknesses are discovered.
3.	Spyware	Spyware can be installed on the computer automatically when the attachments are open, by clicking on links or by downloading infected software.
4.	Ransomware	Ransomware is a type of malicious program that demands payment after launching a cyber-attack on a computer system. This type of malware has become increasingly popular among criminals and costs the organizations millions each year.

Cyber Security Threats

In recent years, most of the individuals and enterprises are facing problems due to the weaknesses inherent in security systems and compromised organizational infrastructures. Different types of Cyber Security Threats are categorized as below:

Phishing

Phishing is a type of computer crime used to attack, steal user data, including login name, password and credit card numbers e.t.c. through emails.

Pharming

Pharming is a scamming practice in which malicious code is installed on a personal computer or server, misdirecting users to fraudulent web sites without their knowledge or permission. Pharming has been called "**phishing without a trap**". It is another way hackers attempt to manipulate users on the Internet. It is a cyber-attack intended to redirect a website's traffic to a fake site.

Cookies

A cookie is a small piece of data sent from a website and stored on the user's computer memory (Hard drive) by the user's web browser while the user is browsing internet.

Web sites typically use cookies for the following reasons:

- To collect demographic information about who has visited the Web site.
- Sites often use this information to track how often visitors come to the site and how long they remain on the site.

Firewall and Proxy Servers

A firewall is a computer network security based system that monitors and controls incoming and outgoing network traffic based on predefined security rules. A firewall commonly establishes a block between a trusted internal computer network and entrusted computer outside the network.

A proxy server acts as an intermediary between the end users and a web server. The proxy server examines the request, checks authenticity and grants the request.

Encryption and Decryption

Encryption and decryption are processes that ensure confidentiality that only authorized persons can access the information.

Encryption is the process of translating the plain text data (plaintext) into random and mangled data (called cipher-text).

Decryption is the reverse process of converting the cipher-text back to plaintext.Encryption and decryption are done by cryptography. In cryptography a key is a piece of information (parameter) that determines the functional output of a cryptographic algorithm.

Encryption is used to protect data in communication system, for example data being transferred via networks (e.g. the Internet, ecommerce), mobile telephones, wireless microphones, wireless intercom systems, Bluetooth devices and bank automatic teller machines.

17.4 INTRODUCTION TO INFORMATION TECHNOLOGY ACT

In the 21st century, Computer, Internet and ICT or e-revolution has changed the life style of the people. Apart from positive side of e-revolution there is also negative side of computer, that

is, the internet and ICT in the hands of criminals .To tackle the problems of cyber crimes Cyber Law or Cyber Space Law or Information Technology Law or Internet Law were introduced.

In India Cyber law and IT Act 2000 , modified in 2008 are being articulated to prevent computer crimes. IT Act 2000 is an act to provide legal recognition for transactions carried out by means of **ElectronicData Interchange(EDI)** and other means of electronic communication. It is the primary law in India dealing with cybercrime and electronic commerce(e-Commerce). e-Commerce is electronic data exchange or electronic filing of information.

PREVENTION

25% of cyber crime remains unsolved. To protect the information the following points are to be noted:

- Complex password setting can make your surfing secured.
- When the internet is not in use, disconnect it.
- Do NOT open spam mail or emails that have an unfamiliar sender.
- When using anti-virus software, keep it up-to-date.

Evaluation

PART - I

Choose the best Answer.

FDYPN3

1. Which of the following is a set of moral principles that regulate the use of computers ?

   a. piracy b. programs
   c. virus d. computer ethics

2. Commercial programs made available to the public illegally are known as

   a. freeware b. warez
   c. free software d. software

3. Which one of the following are self-repeating and do not require a computer program to attach themselves?

   a. viruses b. worms
   c. spyware d. Trojans

4. Which one of the following tracks a user visits a website?

   a. spyware b. cookies
   c. worms d. Trojans

5. Which of the following is not a malicious program on computer systems?

   a. worms d. Trojans
   c. spyware d. cookies

6. A computer network security that monitors and controls incoming and outgoing traffic is

   a. Cookies b.Virus
   c. Firewall d. worms

7. The process of converting cipher text to plain text is called

   a. Encryption b. Decryption
   c. key d. proxy server

8. e-commerce means

   a. electronic commerce
   b. electronic data exchange
   c. electric data exchange
   d. electronic commercialization.

9. Distributing unwanted e-mail to others is called.

   a. scam b. spam
   c. fraud d. spoofing

10. Legal recognition for transactions are carried out by
    a. Electronic Data Interchange
    b. Electronic Data Exchange
    c. Electronic Data Transfer
    d. Electrical Data Interchange

Part – II

Very Short Answers

1. What is Harvesting ?
2. What are Warez?
3. Write a short note on cracking.
4. Write two types of cyber attacks.
5 . What is a Cookie?

Part-III

Short Answers

1. What is the role of firewalls?
2. Write about encryption and decryption.
3. What are the guidelines to be followed by any computer user?
4. What are ethical issues? Name some.

Part –IV

Explain in Detail

1. What are the various crimes happening using computer?
2. What is piracy? Mention the types of piracy? How can it be prevented?
3. Write the different types of cyber attacks.

Reference :

- Computer Network Security and Cyber Ethics by Joseph MiggaKizza
- "Investigating Cyber Law and Cyber Ethics: Issues, Impacts and Practices: 1" by Alfreda Dudley and James Braman

GLOSSARY

WORD	***MEANING***
Authenticity	The quality of being real or true.
Computer Crime	Computer crime is an intellectual crime to manipulate computer system.
Ethics	Moral principles that govern a person's behaviour or the conducting of an activity.
Hacking	Hacking is gaining unauthorized access to computer system without the owner's permission.
Perpetrator	A person who carries out a harmful, illegal, or immoral act.
Software Piracy	Software Piracy is the copyright violation of software created originally by one person and illegally used by someone else.