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.

FDTGAC

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. They play an important role in the daily lives of individuals and businesses. 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 and is caused by criminals or irresponsible action of individuals who are exploiting the widespread use of Internet. It presents a major challenge to the ethical use of information technologies. Cyber-crime also poses threats to the integrity, safety and survival of most business systems.

Figure. 17.1 presents the types of cyber-crimes that happen across the world.

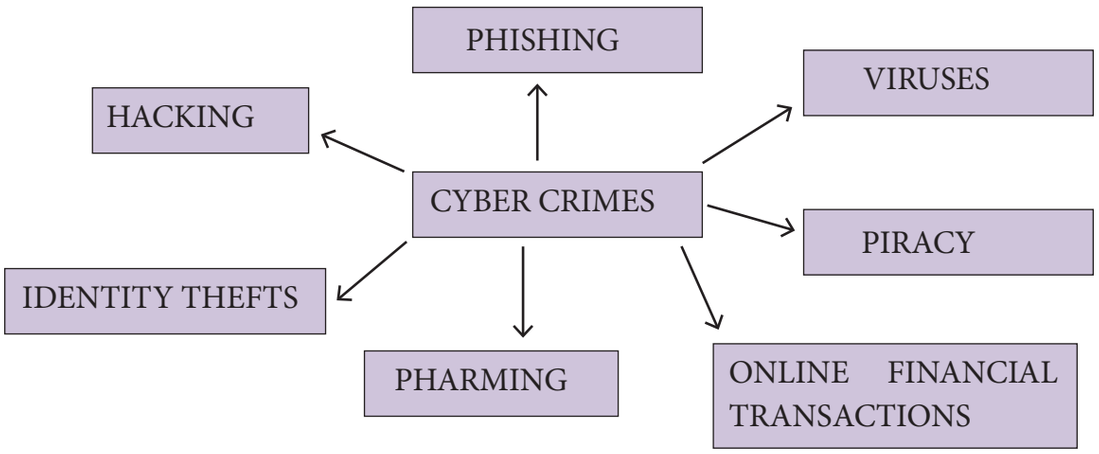

Figure 17.1 Types of cyber – crimes

ETHICS

Ethics means "What is wrong and What is Right". It is a set of moral principles that rule the behavior of individuals who use computers. An individual gains knowledge to follow the right behavior, using morals that are also known as ethics. Morals refer to the generally accepted standards of right and wrong in the society. Similarly, in cyber-world, there are certain standards such as

- Do not use pirated software
- Do not use unauthorized user accounts
- Do not steal others' passwords
- Do not hack

The core issues in computer ethics are based on the scenarios arising from the use of internet such as privacy, publication of copyrighted content, unauthorized distribution of digital content and user interaction with web sites, software and related services.

COMPUTER ETHICS

With the help of internet, world has now become a global village. Internet has been proven to be a boon to individuals as well as various organizations and businesses. e-Commerce is becoming very popular among businesses as it helps them to reach a wide range of customers faster than any other means.

Computer ethics deals with the procedures, values and practices that govern the process of consuming computer technology and its related disciplines without damaging or violating the moral values and beliefs of any individual, organization or entity.

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. **Professionalism:** Each user should maintain professional conduct.

5. **Obey The Law:** Users should strictly obey the cyber law in computer usage.

6. **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
- Unauthorized Access
- 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
Cyber Terrorism	Hacking, threats, and blackmailing towards a business or a person.
Cyber stalking	Harassing through online.
Malware	Malicious programs that can perform a variety of functions including stealing, encrypting or deleting sensitive data, altering or hijacking core computing functions and monitoring user's computer activity without their permission.
Denial of service attack	Overloading a system with fake requests so that it cannot serve normal legitimate requests.
Fraud	Manipulating data, for example changing the banking records to transfer money to an unauthorized account.
Harvesting	A person or program collects login and password information from a legitimate user to illegally gain access to others' account(s).
Identity theft	It is a crime where the criminals impersonate individuals, usually for financial gain.
Intellectual property theft	Stealing practical or conceptual information developed by another person or company.
Salami slicing	Stealing tiny amounts of money from each transaction.
Scam	Tricking people into believing something that is not true.
Spam	Distribute unwanted e-mail to a large number ofinternet users.
Spoofing	It is a malicious practice in which communication is send from unknown source disguised as a source known to the receiver.

SOFTWARE PIRACY

Software Piracy is about the copyright violation of software created originally by an individual or an institution. It includes stealing of codes / programs and other information illegally and creating duplicate copies by unauthorized means and utilizing this data either for one's own benefit or for commercial profit.

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

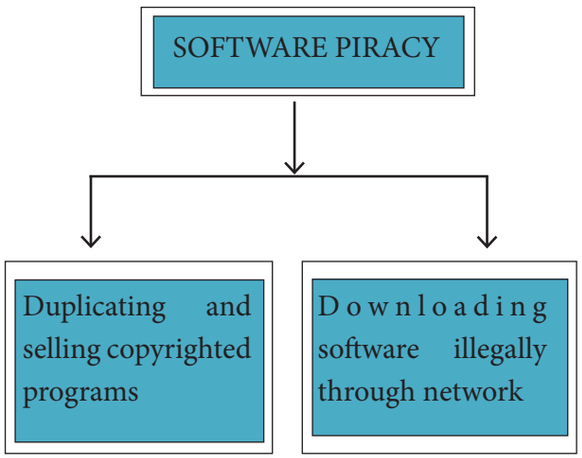

Figure 17.2- Diagrammatic representation of Software piracy

An entirely different approach to software piracy is called **Shareware**, this acknowledges the futility of trying to stop people from copying software and instead relies on people's honesty. 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**.

UNAUTHORIZED ACCESS

Unauthorized access is when someone gains access to a website, program, server, service, or other system by breaking into a legitimate user account. For example, if someone tries guessing a password or username for an account that was not theirs until they gained access, it is considered an unauthorized access.

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

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.

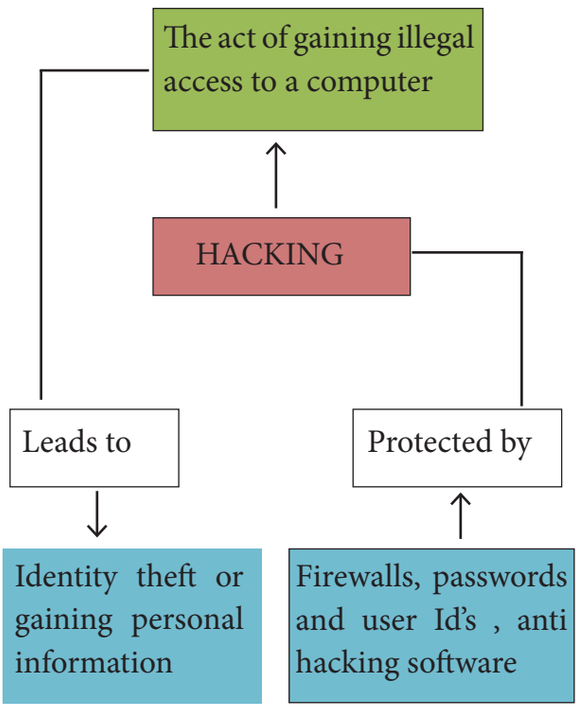

Figure 17.3 Diagramatic representation of Hacking

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

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.

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. It occurs when an attacker targets a victim into opening an e-mail or an instant text message. The attacker uses phishing to distribute malicious links or attachments that can perform a variety of functions, including the extraction of sensitive login credentials from victims.

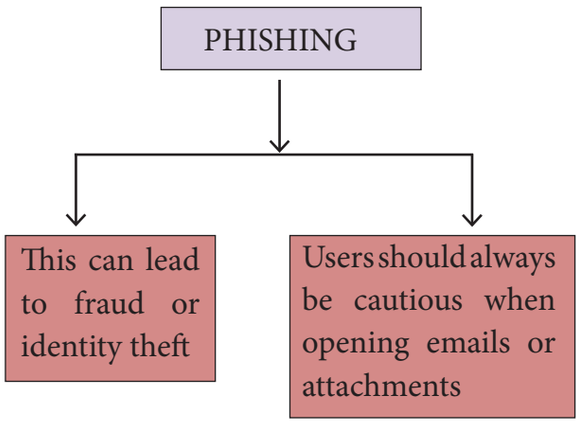

Figure 17.4 Diagrammatic representation of Phishing

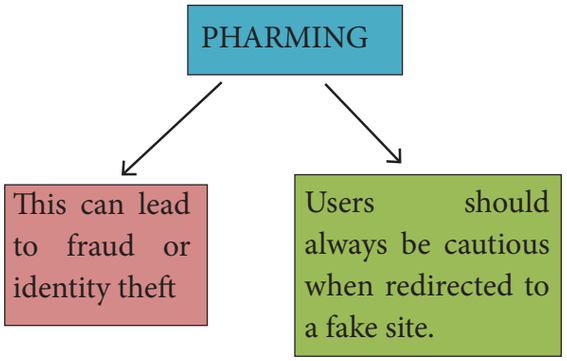

Figure 17.5 Diagrammatic representation of Pharming

Man In The Middle (MITM)

Man-in-the-middle attack (MITM; also Janus attack) is an attack where the attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other.

Example: Suppose Alice wishes to communicate with Bob. Meanwhile, Mallory wishes to intercept the conversation to overhear and optionally to deliver a false message to Bob.

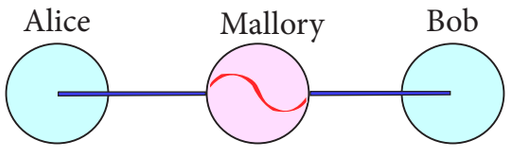

Figure 17.6 - An illustration of the Man-In-The-Middle attack

Cookies

A cookie (also called HTTP cookie, web cookie, Internet cookie, browser cookie, or simply 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. Cookies were designed to be a reliable mechanism for websites to remember stateful information (such as items added in the shopping cart in an online store) or to record the user's browsing activity (including clicking particular buttons, logging in etc.). They can also be used to remember arbitrary pieces of information that the user previously entered into form fields such as names, addresses, passwords, and credit card numbers. From the security point of view, if cookie data is not encrypted, any anonymous user (hacker) can access the cookie information and misuse it.

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.
- It helps to personalize the user's experience on the Web site.
- Cookies can help store personal information about users so that when a usersubsequently returns to the site, a more personalized experience is provided.

If you ever returned to a site and have seen your name mysteriously appear on the screen, it is because on a previous visit, you gave your name to the site and it was stored in a cookie. A good example of this is the way some online shopping sites will make recommendations to users based on their previous purchases. It helps to monitor advertisements. Cookies do not act maliciously on computer system. They are merely text files that can be deleted at any time.

Cookies cannot be used to spread viruses and they cannot access your hard drive. However, any personal information that you provide to a Web site, including credit card information, will most likely be stored in a cookie unless the cookie feature is explicitly turned off in your browser. This is the way in which cookies threaten privacy.

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. **Figure 17.7** shows the working of firewall server.

A proxy server acts as an intermediary between the end users and a web server. A client connects to the proxy server, requesting some service, such as a file, connection, web page, or other resources available from a different server. The proxy server examines the request, checks authenticity and grants the request based on that. Proxy servers typically keep the frequently visited site addresses in its cache which leads to improved response time. **Figure 17.8** shows the working of a proxy server.

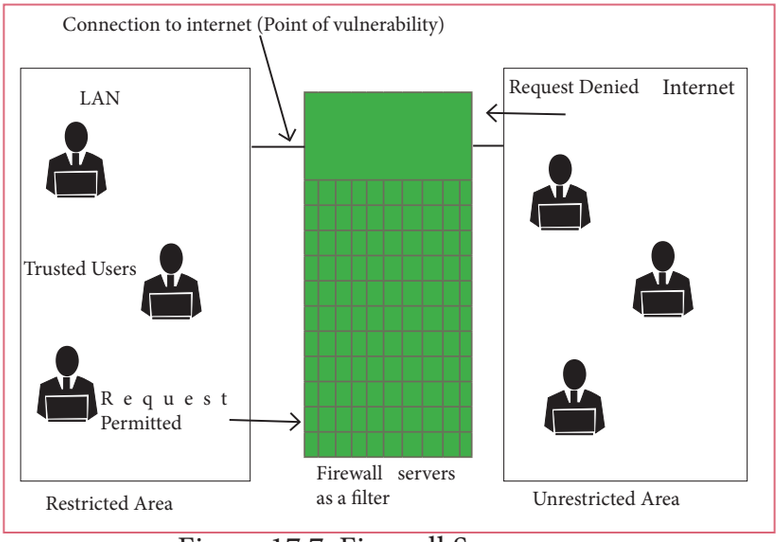

Figure 17.7 Firewall Server

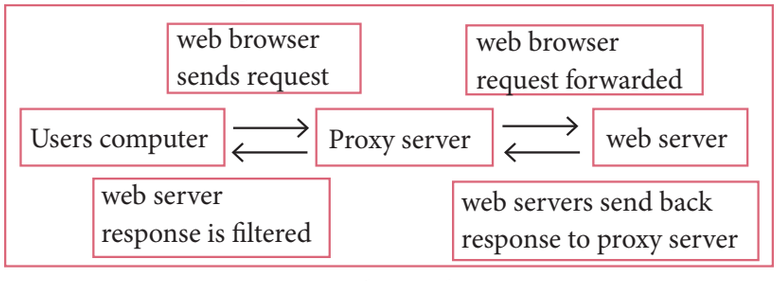

Figure 17.8 Working of Proxy server

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.

Figure 17.9 shows the encryption and decryption process.

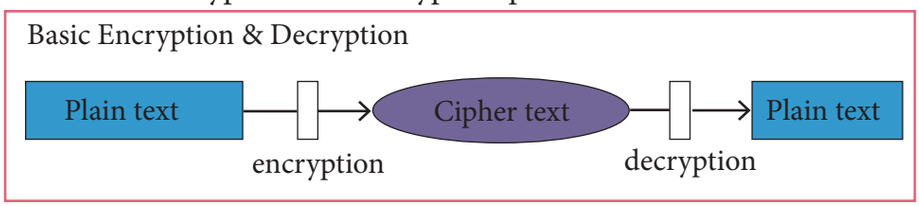

Figure 17.9 Encryption and Decryption

Encryption has been used by militaries and governments to facilitate secret communication. It is now commonly used in protecting information within many kinds of civilian systems. It is also 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. There have been numerous reports of data in communication being intercepted in recent years. Data should also be encrypted when transmitted across networks in order to protect against the network traffic by unauthorized users.

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. Today paper based communication has been substituted by e-communication. Accordingly we have new terminologies like cyber world, e-transaction, e-banking, e-return and e-contracts. 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 which has become a weapon of offence. Accordingly a new panel of members emerged to tackle the problems of cyber crimes in cyber space i.e. Cyber Law or Cyber Space Law or Information Technology Law or Internet Law.

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.

"Cyber law or Internet law is a term that encapsulates the legal issues related to use of the Internet.

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.

- Awareness is the key to security.
- Information security is the immune system in the body of business.
- A check that does not bounce is called the Security Check. Do it every day before you leave!
- Do Your Part - Be Security Smart !!!
- Don't be Quick to Click… be wary when you shop online.
- Restart is Smart job
- Passwords are like toothbrushes. They are best when new and should never be shared.
- When you and your system part away, your system should be first off for the day.
- Your mind is a storage room of information, keep the door locked.
- _ a _ _word is not a PaSSword without Protect, Save and Secure!
- Link Link stop neglect….Think Think before connect…..

Evaluation

SECTION – A

Choose the correct answer

1. Which of the following deals with procedures, practices and values?
   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

SECTION-B

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?

SECTION-C

Short Answers

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

FDYPN3

SECTION - D

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 Books :

- 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