Tehkals.com
Learn & Teach

CLASS 9

Computer Notes

Chapter No. 6

NAME: _____

F.NAME: _____

CLASS:_____ SECTION: _____

ROLL #: _____ SUBJECT: _____

ADDRESS: _____

_____

SCHOOL: _____

UNIT: 6
COMPUTER SECURITY AND ETHICS

Q.3 Give short answers to the following questions.

(i) What is computer security?

Ans: COMPUTER SECURITY:

Computer security is a branch of computer technology known as information security as applied to computers and networks. The objective of computer security includes protection of information and property from theft, corruption, or natural disaster. It allows the information and property to remain accessible and productive to its intended users.

(ii) What is the difference between a computer crime and a conventional crime?

Cyber crime

Cybercrime refers to any crime committed using the means of technology and the internet performed by expert user. The methods that cyber criminals use to gather data and perform an attack is comparable to physical 'traditional' crimes

Conventional crime

Conventional crimes are those traditional, illegal behaviors that most people think of as crime. Most crime is conventional crime

iii. Differentiate between hacking and cracking.

HACKING:

Hacking is gaining unauthorized access to computers or telecommunications systems.The professionals, who do hacking, are called hackers. Sometimes hacking is done as a service to expose security flaws to companies or organizations.

CRACKING: Software cracking is the process of bypassing the registration and payment options on a software product to remove copy protection safeguards or to turn a demo version of software into a fully functional version without paying for it. The people who do cracking are called crackers.

iv. What is the difference between a virus and a worm?

Ans:

VIRUS	WORM
It damages your data or interfere normal operations of your computer.	It uses computer network to replicate it self
It may format your hard disk	It reduces your computer memory or disk apace
It harms your computer without your knowledge	Worm normally infects other computer through computer network
Computer viruses are usually men-made	It spread from computer to computer without any human action
Virus needs a host program to run	Worm can run it self

v. What is adware? How a user can get rid off and remove adware?

Ans: ADWARE: Adware is advertising-supported software, which gets the online ads to play automatically. It downloads itself without users' knowledge or permission. These programs overload the system and enter a code that could suddenly make the content of the computer open to the world.

vi. How virus spread through internet in computers?

Ans: How virus spread: There are many ways that computer viruses spread. Sometime users know they are infected with a virus and most times they do not know. Spreading of viruses is due to a variety ofmeans:

- Through infected flash drives/CD's
- Through Pirated software
- Via Network and internet
- Through E-mail attachments

vii. Differentiate between authentication and authorization?

AUTHENTICATION:

Authentication is a process to verify the identity of a user to the computer.The system will validate the user identity and then access will be granted. There are many ways of authenticating a user. Like:

- Password based authentication.
- Device based authentication.
- Biometric authentication.

AUTHORIZATION:

Authorization is finding out if the person, once identified, is permitted to have the resource. It is a process that verify the access level of resources being granted. In other words which resource the user want to access and which kind of access he/she is allowed.

viii. Compare authorized access with unauthorized access.

AUTHORIZED ACCESS:

Authorized access is the use of a computer or network with permission

Authorized use is the use of a computer or its data for approved or possibly legal activities.

UNAUTHORIZED ACCESS:

Unauthorized access is the use of computers and network without permission. Unauthorized use of a computer or its data for unapproved or illegal activities.

ix. What is biometrics technology? Give one example.

Ans: BIOMETRICS: This form of authentication provides the physiological makeup of the human body and/or passwords. Today, most laptops come with fingerprint biometrics readers. Biometrics can use physical characteristics, like human face, fingerprints, irises, or behavioral characteristics like human voice, handwriting or typing rhythm. Biometrics uses unique features, like the iris of an eye, to identify a person.

x. What is multimodal authentication?

Ans: MULTIMODAL AUTHENTICATION: Multimodal or multifactor authentication is the act of using more than one authentication method when logging on to a server or a workstation. This form of authentication helps to provide additional security to applications or computers.

The need for Multimodal Authentication has become increasingly necessary as more people conduct transactions online, and as crime rates have made it prudent to secure office buildings so that only authorized personnel may enter.

Q.4 What is importance of computer security?

Ans: IMPORTANCE OF COMPUTER SECURITY: Security of Computer is rapidly gaining importance in today's world where almost every day important confidential online documents and information have the possibility of being stolen online. Computer security generally deals with processes, by which valuable data can be protected and preserved, in both their theoretical and practical aspects. Computer security was introduced in the 1970's. The purpose of computer security is to secure a particular computer system from any king of crime. Computer security, therefore, aims at securing data, keeping them intact and also providing uninterrupted services.

Q.5 What is cybercrime? Explain different types of cybercrime.

Ans: CYBERCRIME: Cybercrime refers to any crime that involves a computer and a network. Cybercrime may include:

- Altering computer input in an unauthorized way.
- Altering, destroying, suppressing, or stealing output, usually to conceal unauthorized transactions.
- Altering or deleting stored data.
- Altering or misusing existing system tools or software packages, or altering or writing code for fraudulent purposes.
- Other forms of fraud may be facilitated using computer systems, including bank fraud, identify theft, extortion, and theft of classified information.

HACKING:

Hacking is gaining unauthorized access to computers or telecommunications systems. The professionals, who do hacking, are called hackers. Sometimes hacking is done as a service to expose security flaws to companies or organizations.

CRACKING:

Software cracking is the process of bypassing the registration and payment options on a software product to remove copy protection safeguards or to turn a demo version of software into a fully functional version without paying for it. The people who do cracking are called crackers.

Q.6 "Virus is a great threat to computers". Why? Explain different types of computer viruses. Ans:

VIRUS:

Computer Virus is a kind of malicious software written intentionally to enter a computerwithout the user's permission or knowledge, with an ability to replicate itself, thus continuing to spread. Some viruses do little but others can replicate and cause severe harm or adversely affect program and performance of the system. A virus should never be assumed harmless and left on a system. Most commontypes of viruses are mentioned below:

Resident Viruses:

This type of virus is a permanent which dwells in the RAM memory. It corrupts filesand programs that are opened, closed, copied, renamed etc.

Boot Virus:

This type of virus affects the boot sector of a hard disk, which is a crucial part of a disk.

Trojans or Trojan Horses:

A Trojan or Trojan horse is a destructive program that disguises itself asvaluable and useful software available for download on the internet. Unlike viruses or worms, Trojans do not replicate themselves, but they can be just as harmful as viruses of worms.

Logic Bomb or Time Bomb Virus:

A logic bomb is a piece of code intentionally inserted into softwarethat will set off a malicious function when specified conditions are met. For example, a programmer may hide a piece of code that starts deleting files from company's database.

Sir Cam:

An e-mail virus travels as an attachment to e-mail messages, and usually replicates itself by automatically mailing itself to dozens of people in the victim's e-mail address book.

Q.7 Differentiate between malware and spyware.

MALWARE:

Mal-ware stands for malicious software that includes computer viruses, worms, Trojan, horses, spyware, dishonest adware, and other malicious from web sites, and virus-infected files downloaded from peer-to-peer connections. Malware works to remain unnoticed, either by actively hiding or by simply not making its presence on a system known to the user.

SPYWARE:

Spyware are malicious programs that collect various types of personal information, such as internet surfing habits and sites that have been visited by users. They also interfere with users' control of the computer in other ways, such as installing additional software and redirecting web browser activity. Spyware have capabilities to change computer settings, resulting in slow connection speeds, different home pages, and/ or loss of internet connection or functionality of other programs.

Q.8 What are different ways of spreading virus in computers?

Ans: How virus spread: There are many ways that computer viruses spread. Sometime users know they are infected with a virus and most times they do not know. Spreading of viruses is due to a variety ofmeans:

- Through infected flash drives/CD's
- Through Pirated software
- Via Network and internet
- Through E-mail attachments

(a) **THROUGH INFECTED FLASH DRIVES/CD'S:** These are most common ways of virus spreading from one computer to the other. Through an infected computer, and using a CD/DVD or Flash drive, virus can easily be copied on them.

(b) **THROUGH PIRATED SOFTWARE:** Pirated software is unauthorized copy of legitimate software. Gaining illegal access to protected software by any means is also known as software piracy. Pirated software usually contains viruses.

(c) **VIA NETWORKS AND INTERNET:** Files shared on a network and downloaded directly from the internet (either through file-sharing programs or direct download from websites), are among the fastest growing sources of computer virus infections.

(d) **THROUGH E-MAIL ATTACHMENTS:** Most of the viruses that spread on the computer are delivered through attachments. These attachments are sent via email most often from people you know. E-mails infected with a virus usually appear like any normal email in the inbox. When the user opens the email and the attachment, the virus executes itself and will erase or change information.

Q.9 How a computer virus affects a computer system? Elaborate your answer by listing various symptoms of an attack by viruses.

Ans: Computer viruses used to spread by disk. But as the internet became popular, viruses started spreading faster by e-mail. To prevent damages, virus protection and removal programs (Anti-viruses) mustbe installed.

SYMPTOMS OF A VIRUS ATTACK: Here are a few symptoms/indicators that indicate the computer might be infected with a virus:

- The computer runs more slowly than normal.
- The computer stops responding or freezes often.
- The computer crashes and restarts every few minutes.
- The computer restarts on its own and then fails to run normally
- Applications on the computer do not work correctly.
- Disks or disk drives are inaccessible.
- Users can not print correctly.
- Users can see unusual error messages.
- Users see unreadable menus and dialog boxes.

These are common signs of virus infection- but they might also indicate hardware or software problems that have nothing to do with a virus. Unless users install up-to-date antivirus software on their computers, there is no way to be certain if the computer is infected with a virus or not.

Q.10 How a computer can be protected against virus?

Ans: To prevent damages, virus protection and removal programs have become compulsory for the computer systems. Because new viruses are created constantly, virus protection is never guaranteed, but updated virus protection software is preferred. Antivirus and Antispyware software are a necessity today to ensure the security of the computer and personal information.

1. **ANTIVIRUS:** Antivirus is programs which are capable of locating, preventing, and removing the malicious programs from a computer system. Antivirus Software, as the name itself suggests, have proved to be a very useful means of protecting computer systems from harmful viruses and worms, thereby, providing protection to the computer systems. Hence, it is essential to update Antivirus Software's on a regular basis so as to keep a computer system safe from viruses.
2. **ANTI SPYWARE:** Antispyware software protects the computer against pop-ups, slow performance, and security threats caused by spyware and other unwanted software. To keep protecting from the latest spyware, users must keep the antispyware software updated.
   Microsoft Security Essential is a new, free consumer anti-malware solution for computers. It helps protect against viruses, spyware, and other malicious software. It is available as a no-cost download for Windows XP SP2 and higher, Windows Vista, and Windows 7.

Q.11 Explain different Authentication Methodologies in detail.

Ans: **AUTHENTICATION METHODOLOGIES:** The following are few important authentication methodologies that can be used according to the needs of users or organizations.

1. **USERNAME AND PASSWORD:** In this method username and password is used for authentication. The username usually reflects the name of the individual. Passwords need to be complex. Passwords should not be written down or shared.
2. **PERSONAL IDENTIFICATION NUMBER (PIN):** A personal identification number (PIN, pronounced "pin") is a secret numeric password shared between a user and a system that can be used to authenticate the user to the system. Typically, the user is required to provide a non-confidential user identifier or token (the user ID) and a confidential PIN to gain access to the system. PINs aremost often used for automated teller machines (ATMs) but are increasingly used at the point of sale, for debit cards and credit cards.
3. **ACCESS CARDS:** Access cards or security pass cards are often used to gain entry into areas and buildings with restricted access. The access cards may be for general access, meaning that the car does not provide data about the person using it, or it may be individually encoded, containing specific information about the cardholder.

   Typically, the data on an encoded security cards includes:
   - Name
   - ID # (social security number or other unique number)
   - Access level (where you're allowed to go)
   - A card reader can understand the information on the card.
4. **BIOMETRICS:** This form of authentication provides the physiological makeup of the human body and/or passwords. Today, most laptops come with fingerprint biometrics readers. Biometrics can use physical characteristics, like human face, fingerprints, irises, or behavioral characteristics like human voice, handwriting or typing rhythm. Biometrics uses unique features, like the iris of an eye, to identify a person.

Q.12 What are computer ethics? Give a sample code of conduct suggested by the Computer Ethics Institute (CEI).

Ans: **COMPUTER ETHICS:** Computer ethics are the issues concerning the legal, professional, social, and moral responsibilities of computer professional and end users. Basically, Computer ethics are, just knowing the difference between ethical and unethical. For example, while it is easy to duplicate copyrighted electronic

(or digital) content, computer ethics would suggest that it is wrong to do so without the authors' or owners' approval. And while it may be possible to access someone's' personal information on a computer system, computer ethics would advise that such an action is unethical.

MORAL GUIDELINES FOR THE USE OF COMPUTERS: A sample code of conduct suggested by the computer ethics Institute is listed below as guidelines for the use of computers:

1. Do not use computer to harm other people.
2. Do not snoop around in other people's computer files.
3. Do not use a computer to steal.
4. Do not use a computer to bear false witness.
5. Do not copy or use proprietary software for which you have not paid.
6. Do not use other people's computer resources without authorization or proper compensation.
7. Always think about the social consequences of the program you are writing or the system you are designing.
8. Always use a computer in ways that ensure consideration and respect for your fellow humans.

Q.13 Explain different areas of computer ethics.

Ans: AREAS OF COMPUTER ETHICS: The following are few major areas of computer ethics.

- Information Accuracy
- Copyright and intellectual property rights
- Software Piracy
- Information Privacy

a. INFORMATION ACCURACY: Information accuracy concerns with the correct handling of 'personal information', that is, information about a particular person or organization to identify their particulars to other. The accurate use of such information is essential to businesses, non-profit organizations, consumers and government. Information can be shared and used by more than one person at the same time, and it can be used for an unlimited number of different purposes. These characteristics give rise to the fundamental ideas behind information accuracy.

b. Copyright and intellectual property rights: Property generally used to mean a possession, or more specifically, something to which the owner has legal rights. You might have also encountered the phrase intellectual property. This term has become more commonplace during the past few years, especially in the context of computer ethics. Intellectual property refers to creations of the intellect. It may include inventions, literary and artistic works, symbols, names, images, and designs, etc. Intellectual property is usually divided into two branches, namely **industrial property** and **copyright**.

c. Software Piracy: Software piracy is the illegal copying of the copyright or licensed software. In this a licensed copy of software is purchased and then a large number of copies of this software are prepared and sold in the market. Software piracy is morally bad when someone reproduces a copy of the software and sells it for profit, produces exactly the same or similar version without giving proper credit to the original author.

d. Information Privacy: Information privacy, also called data privacy is the relationship between collection and distribution of data, technology and the other issues related to them.

Data privacy issues can arise in response to information from a wide range of sources, such as:

- Healthcare records.
- Criminal justice investigations and proceedings.
- Financial institutions and transactions.
- Biological traits, such as genetic material.
- Residence and geographic records.
- Ethnicity.

The challenge in data privacy is to share data while protecting personally identifiable information and not to misuse or mishandle it.

Q.14 Why antivirus software is necessary for a computer?

Ans: ANTIVIRUS: Antivirus is programs which are capable of locating, preventing, and removing the malicious programs from a computer system. Antivirus Software, as the name itself suggests, have proved to be a very useful means of protecting computer systems from harmful viruses and worms, thereby, providing protection to the computer systems. Hence, it is essential to update Antivirus Software's on a regular basis so as to keep a computer system safe from viruses.

INSTALLING ANTIVIRUS: Antivirus is essential software for every computer system. Antivirus protects computer from many common viruses and Trojans which can be harmful for the system. Avast Antivirus (Free Edition) is very good and effective FREE Antivirus.