

FOUNDATION OF INFORMATION TECHNOLOGY
SOCIETAL IMPACTS OF IT
CHAPTER 10

Ans1. Hacking refers to gain unauthorized access to computer system for the purpose of stealing and corrupting data. There have been several instances where hacking has proven to have caused problems.

Ans2. Different forms of attacks that generally takes place are:-

- a. Spamming
- b. Computer viruses
- c. Spyware
- d. Worms
- e. Trojan horses
- f. Sweeper
- g. Phishing etc

Ans3. Spamming refers to the sending of bulk-mail by an identified or unidentified source. The attacker keeps on sending bulk mail until the mail server runs out of disk space.

Ans4. Computer Viruses: Computer viruses are the malicious codes/programs that cause damage to data and files on a system. Viruses can attack any part of computer software such as boot block, operating system, system area, files and application programs. Different types of viruses are: File infectors, Boot sector and Macro viruses.

Worm: A worm is a self replicating program which eats up the entire disk space or memory. A worm keeps on creating its copies until the disk space or memory is filled.

Trojan Horses: A Trojan horse is a program that appears harmless but actually performs malicious function such as deleting or damaging files.

Sweeper: This is another malicious program used by crackers. It sweeps or deletes all the data from the system.

Malware: Malware is a general term used to refer to viruses, worms, spyware, adware etc. These are unwanted software that someone else wants to run on your computer. They infect our system and behave in a way which we never want to be like this.

Adware: These are the program that delivers unwanted ads to your computer. They consume your network bandwidth. They appear generally in pop-ups form.

Spyware: Spyware is software which is installed on your computer to spy on your activities and report data to people willing to pay for it. Spyware can be used either for legal or illegal purpose to spy on computer activities.

Ans5. This type of attack eats up all the resources of a system and the system or applications come to a halt. Due to this we will not be able to use available services of computer. It may be done by virus by deleting system files or spamming etc due to which the services turn to stop working.

Ans6. It is the criminally fraudulent process of attempting to acquire sensitive information such as user name, password, credit card information, account data etc. Here an imposter uses an authentic looking email or website to trick recipients into giving out sensitive personal information. You may receive an authentic looking email or webpage to trick out your confidential data which may be used later on for cyber crime or fraud.

Ans7. Antivirus software covers the following main lines of attacks:-

- a. It scans incoming emails.
- b. It checks the opened or created files to make sure that they are virus free.
- c. It performs periodic scans.

Ans8. Hacker is a person who enjoys learning programming language and computer systems and can be considered an expert on the subject.

The crackers are the malicious programmers who break into secure systems and can cause severe damage to our system whereas hackers are more interested in gaining knowledge about computer system and using this knowledge for playful pranks.

Ans9. A copy of data that can be used to restore and recover the data after failure is called a backup. It is required to take backup of your important data against many failures such as:

- a. Hardware failure
- b. Media failure
- c. Accidental deletion of data
- d. Theft and natural disaster
- e. Virus attack

Ans10. We can have two ways to take backups:

- a. **Full backup:-** is a method of backup where all the files and folders selected for the backup will be backed up. It is commonly used as an initial or first backup followed with subsequent differential backups. After several incremental/differential backups, it is common to start over with a fresh full backup again.
- b. **Differential backup:-** is based on the latest full backup of the data. This is known as differential base. A differential base is a full backup of data. A differential backup contains only the data that has changed since the differential base. Differential backup that are taken fairly soon after the base backup are smaller and faster and decrease the risk factor of data loss. Several successive differential backups use one differential base.

Ans11. Online backup is a way of storing data on remote (offsite) server or computer with network connection. In case of data loss in any ways, you simply have to connect to remote computer to restore it and thus we can access our data from anywhere and at any time.

There are many advantages of online backup over traditional backups

- a. Less risk factor of data loss.
- b. Safety of data.
- c. No need to maintain any extra hardware.
- d. Automatic Data backup facility.
- e. Data is available anywhere and at any time.

Ans12. Already Covered in Ans11

Ans13. Some E-commerce security provisions are:-

- a. Encryption
- b. Digital Signature
- c. Digital Certificate
- d. SSL(Secure Socket Layer)
- e. PCI(Peripheral component interconnect)
- f. SET(Secure Electronic Transaction)
- g. Firewall
- h. Kerberos etc

Ans14. Digital Signature:- A digital Signature is a digital code attached to an electronically transmitted message that uniquely identifies the sender. Its purpose is to guarantee that the individual sending the message really is who he or she claim to be.

Digital Certificate:- Digital certificate is a digital document issued by CA(certification Authority: verisign, Thawte etc). Digital certificate are sold for emails, e-merchants and web servers.