Quize file cs204 created by Toseef
Maryam

Lecture No 4

1. Cyber security refers to the technologies and processes designed to protect computers, networks and data from unauthorized access and attacks delivered through the Internet by cyber criminals.
2. Protecting computer system and information from unauthorized access or destruction / abuse.
3. Security deal with three primary issues, called the CIA triad.
4. Confidentiality Assurance that only authorized user may access a resource.
5. Integrity Assurance that resources has not been modified.
6. Availability Assurance that authorized user may access a resource when requested.
7. Protecting information in the digital age requires constant caution to deter thieves who would steal financial, proprietary, and personal identification data.
8. Cyber security is necessary since it helps in securing data from threats such as data theft or misuse, also safeguards your system from viruses.
9. Security measures provides full security services to balance the needs of providing information to those who need it with taking action to mitigate the dynamic threats posed by cyber thieves and cyber terrorists.
10. Your home computer is the popular target for intruders.
11. We can use our computers to attack other computers on the internet.
12. Intruder attacks home computer because it is not very secure and easy to break into.
13. They do attack your computers by send us a E-mail with virus.
14. Trojan horses are such programs which are used as the back doors.
15. A Virus is a "program" that is loaded onto your computer without your knowledge and runs against your wishes.

16. Virus can reach to our computer through CD-Rom.
17. Virus can reach to our computer through E – mail.
18. Virus can reach to our computer through Websites.
19. Virus can reach to our computer through download files.
20. Install a security suite that protects the computer against threats such as viruses and worms.
21. Handle E- mail attachments carefully.
22. A person who secretly gets access to a computer system in order to get information, cause damage, etc.
23. Hackers attack where they see weakness.
24. A system that hasn't been updated recently has flaws in it that can be taken advantage of by hackers.
25. Regularly update your operating system.
26. Install Anti virus software's.
27. The word "malware" comes from the term "Malicious software."
28. Malware is any software that infects and damages a computer system without the owner's knowledge or permission.
29. Download an anti-malware program that also helps prevent infections.
30. Activate Network Threat Protection, Firewall, Antivirus.
31. Trojan horses are email viruses that can duplicate themselves, steal information, or harm the computer system.
32. These viruses are the most serious threats to computers.
33. Security suites, such as Avast Internet Security, will prevent you from downloading Trojan Horses.
34. Password attacks are attacks by hackers that are able to determine passwords or find passwords

to different protected electronic areas and social network sites.

35. Maintain current software and updates.

36. Never share passwords .

37. Do not click random links.

38. Do not download unfamiliar software off the Internet.

39. Log out or lock your computer.

40. Remove unnecessary programs or services.

41. Frequently back up important documents and files.

42. Protects system against viruses, worms, spyware and other unwanted programs.

43. Protection against data from theft.

44. Protects the computer from being hacked.

45. Simple and practical prevention methods are explained in the lesson to prevent PCs from infection.