Computer Security:

Computer Security is the protection of computing system and the data is access or stored.

Computer Security is the protection of information system from theft or damage to the hardware, software and the information inside it, as well as from disruption or misdirection of service they provide.

Why is Computer Security Important?

- Enabling people to carry out their jobs, education, and research.
- Supporting critical business process.
- Protecting personal and sensitive information.

Cyber security

Cyber security, also referred to as information technology security, focuses on protecting computers, networks, programs and data from unintended or unauthorized access, change or destruction.

Why is Cyber Security Important?

Governments, military, corporations, financial institutions, hospitals and other businesses collect, process and store a great deal of confidential information on computers and transmit that data across networks to other computers. With the growing volume and sophistication of cyber attacks, ongoing attention is required to protect sensitive business and personal information, as well as safeguard national security.

Advantages of Cyber Security:

- Improved security of cyberspace.
- Increase in cyber defence.
- Increase in cyber speed.
- Protecting company data and information.
- Protects systems and computers against virus, worms, Malware and Spyware etc.
- Protects individual private information.
- Protects networks and resources.
- Fight against computer hackers and identity theft

Disadvantages of Cyber Security:

- It will be costly for average users.
- Firewalls can be difficult to configure correctly.
- Need to keep updating the new software in order to keep security up to date.
- Make system slower than before.

Related posts:

1. Types of Attack
2. Security threats
3. Introduction to network security
4. Intrusion detection tool
5. Categories of security assessments
6. Security terminologies and principals
7. Intoduction to intrusion

8. Intrusion detection tool
9. Categories of security assessments
10. Intrusion terminology
11. Cryptography attacks
12. Cryptography
13. SSH
14. MD5
15. Message digest functions
16. Digital signature
17. Authentication Functions
18. One way hash function
19. Hash function in network web security
20. Digital signature standard
21. SSL Secure socket layer