Network Security

Network security is any activity designed to protect the usability and integrity of your network and data. It includes both hardware and software technologies. Effective network security manages access to the network. It targets a variety of threats and stops them from entering or spreading on your network.

Threats to Network Security:

- Virus
- Worms
- Trojan Horse
- Spams

Virus: These are the malicious code/programs that cause damage to data and files on a system. Virus attach itself to program or file so that it can spread from one computer to another leaving infection as it travels. Some Virus cause only annoying effects like changing desktop icons, etc. while others can damage your hardware, software or files. Almost all Virus are attached to an executable file, it means Virus cannot infect your computer unless you run or open the program/file. It means Computer Virus cannot spread without a human action.

Worms: A worm is a self-replication programs which eats up the entire disk space or memory. A Worm keeps on creating its copies until all the disk space or memory is filled. Worms harm to a computer or a computer network by consuming bandwidth and slow down the network speed. After the worm has infected a system,

it can propagate to other systems via internet or while copying files from one system to another without user interaction.

Trojan Horse: It is a program that appears harmless (such as text editor or a utility program) but actually performs malicious functions such as deleting or damaging files. With help of Trojan, harm that could be done by hacker on target computer systems are:

- Data theft
- Installation of unwanted softwares
- Keystroke logging
- Downloading or uploading of files. And many more...

Spam: Means sending of bulk-mail by an identified or unidentified source. In non-malicious form, bulk advertising mail is sent to many accounts. In malicious form (email bombarding) the attackers keep on sending bulk mail until the mail-server runs out of disk space.

Tips to stay safe online

1. Keep Personal Information Professional and Limited
2. Keep Your Privacy Settings On
3. Practice Safe Browsing
4. Make Sure Your Internet Connection is Secure. Use a Secure VPN Connection
5. Be Careful What You Download

6. Choose Strong Passwords
7. Make Online Purchases from Secure Sites
8. Be Careful of What You Post
9. Be Careful of Who You Meet Online
10. Keep Your Antivirus Program Up to Date
11. Don’t click on any unknown links
12. Shop from secured sites only (https)
13. While using public computer, check for any addition device connected to it or be alert of keylogger software, so for financial transaction prefer to use VIRTUAL KEYBOARD rather than keyboard typing
14. Logout from your account and remove history if you are working on public computer