# INDIAN SCHOOLMUSCAT

## CLASS XI

## INFORMATION TECHNOLOGY(802)

## Chapter - 2 : Networking and Internet

**Teacher:** Saju Jagannath

# Some points to keep in mind…..

- Please avoid login from multiple systems.
- Kindly logout at the end of the session.
- Please turn off your mic and webcam
- If you have any doubt, write in the chat box
- If there is any technical problem, hold on – we will be back
- Since it is a lockdown situation you can use rough notebook or notepad or sheets of paper to take down notes. You may take screenshots during the course of delivery of topics.

# Network Safety Concerns Continued….

**IPR Issues:** The intellectual property is the work produced by a person or an organization using the mind and creativity.

The intellectual property comprises of intangible assets such as literary work, artistic work, a work of music, and an engineering design. Intellectual Property Rights (IPR),are the rights of a person or an organization on intellectual property.

# Network Safety Concerns Continued….

Commonly defined Intellectual Property Rights include patents, copyright, industrial design rights, trade marks, trade dress like visual appearance of a product or its packaging, and trade secrets.

There are various issues concerned with these rights such as piracy of software, plagiarism (presenting the literary work done by someone as own work), trademark violations, patent violations, and copyright violations.

# Network Safety Concerns Continued….

**Hacking:** Hacking may be described as having unauthorized access to someone's computer or computer network for stealing resources such as password or confidential files, or causing harm to network or system.

A hacker identifies the vulnerabilities of the system in order to achieve this.

# Network Safety Concerns Continued….

**A hacker** may be driven by several reasons for doing so such as his/ her own personal interest, as a means of fun, or protest. Hackers are also categorized as good hacker and bad hacker. Bad hacker hacks the system with bad intensions whereas good hacker tries to hack system in order to identify its weaknesses so that they can be isolated. These bad (unethical) hackers are termed crackers, as opposed to good (ethical) hackers.

# Network Security Tools and Services

Since Internet has emerged as a prime tool for sharing resources and accessing data, exponentially growing number of users are using it with both good and bad intentions.

Everyone accessing the Internet needs to be aware of the security issues and take protective measures to address the same. Systems that are used as a tool for accessing Internet can be protected using anti-virus and firewall.

# Network Security Tools and Services continued…

**Protection using Anti-Virus**: Anti-virus is software that aims to protect your system against malicious and potentially unwanted programs. It is responsible for detecting these malicious programs by searching or them, and removing them to keep the system protected. The software operates by maintaining a database of malware definitions, which are automatically updated.

# Network Security Tools and Services continued…

It searches for any malicious program by scanning the files against the stored malware definitions for a match. In case of a match, they are declared as potentially harmful, and are disabled and removed depending upon anti-virus software settings.

# Network Security Tools and Services continued…

**Protection using Firewall :** A firewall aims at protecting the internal network of an organization, home, or individual from malicious traffic from external networks. A router or a computer (often dedicated to serve as a firewall) may be installed between external network and internal network for this purpose. Firewall inspects the network traffic, and allows only that data to pass through the network that does not violate the security constraint.

# Network Security Tools and Services continued…

Hardware firewall in form of router prevents malicious software from entering your network from outside network. However, software firewall installed on personal computer prevents unauthorized access or malwares from gaining access to personal computer. Network firewalls may also encrypt the incoming data by converting it to non readable format, thus, adding further protection.

# Network Security Tools and Services continued…

**Protective Measures while accessing Internet :**

Never click on a suspicious link specified on a web page or send through a mail for which you are not sure about its authenticity.

Make sure that passwords are strong and are changed frequently. Passwords are the means for authenticating users, thereby allowing access to networked systems.

# Network Security Tools and Services continued…

Weak passwords have smaller length and uses small subset of possible characters, and thus, are subjected to be cracked easily.

One should also avoid setting obvious passwords such as names, mobile numbers, or date of birth.

Passwords should be strong having long length and including characters such as numbers and punctuation signs.

# Any Questions?