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 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.

Network Security Tools and Services continued…

Never disclose personal information such as account details, passwords, credit and debit card details, and other valuable information. Also, report phishing issues to the concerned authorities. In case of unsolicited mails, mark them as spam mails.

Network Security Tools and Services continued…

Security of the communication made over the Internet can be indicated by the security of protocol being used. Secured Hyper Text Transfer Protocol (HTTPs) is a secure version used for communication between client and host on the Internet. So, ensure that all communications are secure, especially online transactions.

Network Security Tools and Services continued…

The security of website can be ensured of there is padlock on the left side of address bar.
It indicates that website has a SSL (Secure Socket Layer) digital certificate issued by trusted party which ensures and proves identity of remote host.

Network Security Tools and Services continued…

Ensure that the web browser being used for accessing web is updated and is secure.

Make sure that the website address is properly spelled. Because there may be two websites with almost same name, one being a phishing website.

Network Security Tools and Services continued…

The anti-virus software should be up to date. Delete cookies periodically. A cookie is small piece of information about the client browsing a website. On receiving a request from a client, the server records the client information such as domain name and registration id on the server site in the form of a file or a string.

Network Security Tools and Services continued…

The server sends this cookie along with response requested by the client. At the client side, the browser stores this cookie received from the server in a directory called cookie directory.

By obtaining access to these cookies, hacker may gain unauthorized access to these websites. Thus, cookies should be deleted occasionally along with the temporary files stored on our system during web browsing.

Cyber Security

Cybercrimes are the crimes related to the misuse of computer or Internet such as theft,fraud, and forgery.
The IT act defines cybercrime as *an unlawful act where in the computer is either a tool or a target or both.*
Some of these crimes are mentioned below:

1. Sending spam mails to uninterested recipients.
2. Hacking someone's account or system.

Cyber Security

3. Stealing someone's personal information through phishing.
4. Hosting a site carrying lots of malwares or being a source for spreading them.
5. Harassing someone through mails, messages or social networking.
6. Posting offensive content on any site or sending it to anyone.
7. Defaming someone using Internet.

Cyber Security

8. Forging someone's digital signatures
9. Indulging in fraudulent financial transaction
10. Providing misleading information to clients/ general public through use of Internet resources
11. Intellectual Property theft

Cyber Security

Cyber laws are the laws for systematic use of e-resources, for example, e-business, and serve as a measure against illegal cyber-crime.

Various cyber laws have also been enacted to prevent cyber-crimes and take action against those involved in such crimes.

Cyber Security

These laws define the action that would be taken against people committing the offences. For cyber security, an amendment in IT Act 2000 named Information Technology Amendment Act,2008 was also introduced. The act also defines offences and penalties for cyber-crime. Cyber police is responsible for detecting such crimes and taking the necessary measure against it in accordance with IT Act.

Safe Practices on Social Networking

Social network refers to the network of people interacting and sharing information such as their views, photographs, videos and any other information.

Popular social networking sites include Facebook, LinkedIn, and Twitter. Facebook is social networking site with a purpose to connect with the world around you.

Safe Practices on Social Networking

LinkedIn is a business oriented social networking site that aims to connect people professionally. Twitter is a site where people share their views inform of short messages known as tweets limited to 140 characters.

Safe Practices on Social Networking

Social networking has emerged as an important platform where people bounded geographically by distance can communicate and share their views. Often, people interacting with each other share similar interest.

Any Questions?