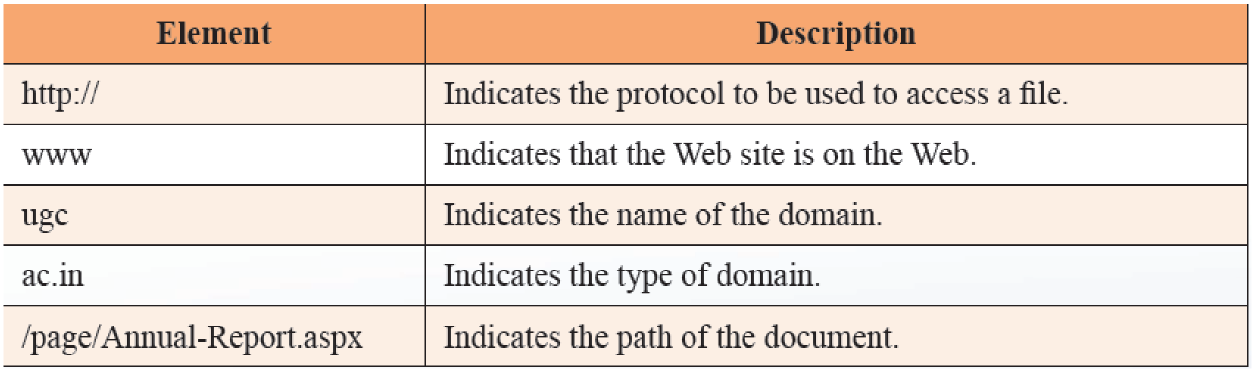
CLASS IX

Session 9

- **Define the term Web, Web browser, Web page, Website, IP address and e-commerce**
- **Ans**:
  - **Web:** The World Wide Web or Web is a way of accessing and sharing information over the Internet by using Web browsers. It is an information-sharing model that is built on top of the Internet. The Web uses the HTTP protocol, only one of the languages used over the Internet, to transmit data. The Web also utilizes browsers, such as Internet Explorer or Firefox, to access Web documents called Web pages that are linked to each other via hyperlinks. The Web refers to the collection of information that is accessible on the Internet.
  - **Web browser:** A Web browser is a software program that enables you to view and interact with various resources on the Web. An example of a widely used Web browser is Microsoft Internet Explorer
  - **Web page:** A Web page is a formatted text document on the Web that a Web browser can display. You can create Web pages by using a software language known as Hypertext Markup Language (HTML).
  - **Website:** A Web site is one or more Web pages that reside on a single server. Every Web site has a unique home page.
  - **IP address:** Each computer on the Web is identified by a unique address, known as the Internet Protocol (IP) address. The IP address is a numeric address that specifies the exact location of a computer on the Web. You can access a computer on the Web by using an IP address, such as 192.168.0.1.
  - **E-commerce:** *E-commerce* refers to the business transactions made over the Internet, such as buying and selling items online.

- Describe the various components of following Uniform Resource Locator(URL) *http://www.ugc.ac.in/page/Annual-Report.aspx*
- **Ans:**

- 

Element	Description
http://	Indicates the protocol to be used to access a file.
www	Indicates that the Web site is on the Web.
ugc	Indicates the name of the domain.
ac.in	Indicates the type of domain.
/page/Annual-Report.aspx	Indicates the path of the document.

Session 10

- **Write the name of various formats for audio files.**

  Ans: Wave (WAV), MPEG Audio Layer 3 (MP3) and Windows Media Audio (WMA)

- **Describe the term speech recognition and speech synthesis.**
- **Ans:** *Speech synthesis* is a technology that allows the computer to speak to you by converting text to digital audio. Windows Vista has a built- in *screen reader* called Narrator that supports speech synthesis. A screen reader is a program that reads the text on the computer screen aloud. To support speech synthesis, your computer must be equipped with a sound card and speakers.
- *Speech recognition* is a technology that allows you to communicate with a computer by using only your voice to enter text and to issue commands. To enable speech recognition, you need an audio input device, such as a microphone, a sound card, and speech recognition software that converts human speech into text or commands for the computer.

- **Describe analog camcorder and digital camcorder**
- **Ans:**

  Analog Camcorder

  An *analog camcorder* records and stores video in an analog format on a tape. To edit the video on a computer, you need to convert it from the analog format to the digital format.

  Digital Camcorder

  A digital camcorder records and stores video in a digital format, which makes editing the recorded video easy. Another advantage is that a digital camcorder is generally lighter and smaller than an analog camcorder.

Session 11

- **Describe computer security and computer privacy.**
- **Ans:**

Computer Security**:** The computer hardware can be damaged due to human carelessness or natural causes. Also, the data and software on the computer need to be protected from accidental or intentional loss and tampering. Computer security deals with the measures that you can take to avoid such damage to the computer and its data

Computer privacy: Computer privacy means that your data, such as personal files and e-mail messages, is not accessible by anyone without your permission. Computer privacy deals with the measures that you can take to restrict access to your data.

- **What do you understand by natural threats? Give any two examples.**

Ans:

Natural calamities such as earthquakes, floods, hurricanes, can damage your computer at any time. Natural calamities can cause fires, extreme temperatures, and lightning strikes that lead to major physical damage to the computers and loss of data.

Following points describe the various natural threats to computer security and privacy.

- Most of the components of a computer are designed to operate within a specific **temperature** range. In case of excessive heat or cold, some components may start to malfunction, and you may need to replace them. If your computer has been exposed to extreme temperatures, let it return to room temperature before you start it.
- **Fire** can damage your computer beyond repair. Even if the computer does not directly catch fire, the heat caused is enough to melt the delicate components inside the computer. Moreover, smoke can damage the CPU fan, which in turn can cause overheating of the CPU and damage it.
- **Lightning** that strikes with a huge amount of electrical charge can cause a surge. A surge or spike is a sudden increase in the supply voltage, which can permanently damage some components of your computer. For example, a sudden increase in voltage can destroy the motherboard of your computer.

- **What do you understand by online predators? Write some guidelines for protection from online predators?**

Ans*:*

- *Online predators* are individuals who lure anybody online, into inappropriate and unethical relationships. You or your family members can become targets of online predators. Online predators develop contact with their targets by using e-mail or chat room communication.

The following points describes the guidelines that you can follow to protect yourself and your family from online predators.

- **Know the signs of predator behavior:** Online predators have some predictable behaviors, which can help you identify them easily. Online predators tend to get intimate very quickly. They often express a great deal of interest and affection toward their targets. You need to ensure that you and your family members can detect such behavior to avoid contact with potential online predators.
- **Be cautious of offers from strangers online:** Online predators usually lure their targets with gifts or other tempting offers. You should be cautious about such gifts or offers. Also, educate your family members to be suspicious about gifts offered over the Internet.
- **Educate your family on online safety measures:** Educate your family members on appropriate chat room behavior to avoid being targeted by online predators. Tell them to use nonsuggestive and neutral screen names. The screen names must not give away their actual name, age, gender, or contact information because this information can be misused.
- **Guide children when they visit Web sites:** As parents, restrict young children from visiting Web sites that are inappropriate for them, or those Web sites that bring them in contact with potential online predators. It is recommended that parents guide their young children when the children visit any Web site. As a parent, instruct your children to leave a Web site if it makes them uncomfortable or if the site contains any unpleasant content. Also, educate your children to leave a Web site that asks for excessive personal information.
- **Know the sites visited by children:** It is important for parents to regularly check the type of Web sites their children visit. You can track the previously visited Web sites by viewing the browser history or by using software that help you track the online activity of a computer.
- **Block access to inappropriate Web sites:** You can enable your browser‟s Content Advisor feature to control the type of Web sites that your family members can visit while browsing the Internet. By using this feature, you can restrict children from visiting Web sites that contain adult content. You can also install certain software programs that help you block specific Web sites.
- **Monitor chat activities:** Specialized software can monitor chat activities and flag inappropriate information exchange on your computer. You can install these software to track the chat activities of your children.

- **Describe the term virus, worm, Trojan horse and spyware**

  Ans:
- ***Viruses*** are computer programs that can damage the data or software on your computer or steal the information stored on your computer. These viruses can reach your computer, without your knowledge, through the Internet or through storage devices, such as floppy disks and CD-ROMs.
- ***Worms*** are viruses that replicate themselves once they attack a computer, making it difficult to remove them. A common worm, known as *Trojan horse* is a kind of virus disguised as useful software. Once a Trojan horse reaches your computer, it starts acting like a virus causing damage to the computer's data.

- ***Spyware*** are programs that get installed on your computer without your knowledge. They can secretly send out information about your Web browsing habits or other personal details to another computer through the network

- **Describe some measures to minimize the risks associated with malicious human threats and human errors.**
  Ans:
- **Store data safely:** Keep your data in safe and secure locations that have limited access to others. This minimizes the possibility of theft or tampering of the data.
- **Encrypt data:** The BitLocker feature of Windows Vista helps you encrypt data at the drive-level. When you encrypt data by using this feature, unauthorized users cannot access the data by removing the hard drive and attaching it to another computer.
- **Install antivirus and antispyware programs:** Antivirus and antispyware software programs have the ability to check for viruses and spyware present in the computer's memory and also prevent new ones from entering. You must regularly update antivirus and antispyware software so that they are able to recognize new viruses and spyware.
- **Install firewall:** Installing a firewall is another effective step that you can take to protect against malicious threats. A *firewall* enables you to filter the Internet traffic before it reaches your computer or a private network. It provides additional protection against threats such as hackers and viruses.
- **Back up data:** Regularly back up important computer data. Creating multiple copies of data provides protection against loss of data due to accidental erasure or destruction of data.