

Chapter 06 – Computer Science (Class 10)

Created by NBF StudyHub (YouTube)

Short Response Questions

1. List the importance of safely use of internet today?

- **Protecting Personal Data:** Safe internet use prevents your personal information (like passwords and bank details) from being stolen by cybercriminals.
- **Preventing Malware:** It helps avoid downloading harmful software (malware) that can damage your device or spy on your activities.
- **Financial Security:** Using the internet safely is crucial for secure online shopping and banking, protecting your money from fraud.
- **Maintaining Privacy:** It ensures that your online interactions and identity remain private and are not exploited by others.

2. State four ways to protect personal information online?

- **Use Strong Passwords:** Create long, complex, and unique passwords for different accounts and consider using a password manager.
- **Be Careful with Sharing:** Limit the personal details you share on social media and think before posting private information.
- **Use Two-Factor Authentication (2FA):** Enable 2FA whenever possible to add an extra layer of security to your accounts.
- **Check Website Security:** Only enter personal information on websites that use 'HTTPS' (look for a padlock icon in the address bar).

3. Mention three benefits of cloud computing?

- **Cost Savings:** You save money because you don't need to buy expensive hardware and software, and you only pay for what you use.
- **Easy Access (Accessibility):** You can access your data and applications from any device, anywhere in the world, as long as you have an internet connection.
- **Automatic Updates & Backup:** The cloud provider manages software updates and automatically backs up your data, so you don't have to worry about losing files.

4. Why is cybersecurity essential in today's digital era?

- **Protecting Data:** Cybersecurity is essential because it shields sensitive personal and business data from theft and unauthorized access by malicious actors.
- **Ensuring System Safety:** It protects computer systems and networks from damage caused by viruses, malware, and hacking attempts.
- **Maintaining Trust:** For businesses, strong cybersecurity builds trust with customers by assuring them that their private information is secure.
- **Preventing Financial Loss:** It helps avoid huge financial losses that can occur due to cyberattacks, fraud, and system downtime.

5. Name three common types of cybercrimes.

- **Phishing:** This is when criminals send fake emails or messages pretending to be a trusted source to trick people into giving away personal information like passwords.
 - **Identity Theft:** This involves stealing someone's personal data (like their name, address, or bank details) to commit fraud or financial crimes in their name.
 - **Malware Attacks:** This is the use of malicious software (like viruses or ransomware) to damage, disable, or gain unauthorized access to a computer system.
-

6. What would you do if your friend faced cyberbullying?

- **Listen and Support:** I would first listen to my friend without judgment and assure them that it is not their fault.
 - **Document Everything:** I would help them take screenshots or save messages as proof of the cyberbullying incidents.
 - **Block and Report:** I would advise them to immediately block the cyberbully and use the reporting features on the social media platform.
 - **Seek Adult Help:** I would strongly encourage and help them to talk to a trusted adult, such as a parent, teacher, or school counselor, for further guidance and action.
-

The End

☒ **Subscribe for Learning**