

CBSE Class 10 Computer Application Question Paper with Solutions(Memory Based)

Time Allowed :3 Hour	Maximum Marks :60	Total Questions :24
----------------------	-------------------	---------------------

General Instructions

Read the following instructions very carefully and strictly follow them:

- Answers to this Paper must be written on the paper provided separately.
- You will not be allowed to write during the first 15 minutes
- This time is to be spent in reading the question paper.
- The time given at the head of this Paper is the time allowed for writing the answers,
- The paper has four Sections.
- Section A is compulsory - All questions in Section A must be answered.
- You must attempt one question from each of the Sections B, C and D and one other question from any Section of your choice.

1. What is the difference between a Web Server and a Web Browser?

Correct Answer: A web server stores and delivers web content, while a web browser is a client application used to access and display that content.

Solution: Concept: The World Wide Web works on a client-server model:

- Web Server → Provides web content
- Web Browser → Requests and displays web content

Step 1: **Web Server.**

- A system that **stores, processes, and delivers web pages.**
- Hosts websites and handles client requests.
- Uses protocols like HTTP/HTTPS.

Examples:

- Apache HTTP Server
- Nginx
- Microsoft IIS

Step 2: **Web Browser.**

- A software application used to **access and view websites**.
- Sends requests to web servers and displays responses.
- Interprets HTML, CSS, and JavaScript.

Examples:

- Google Chrome
- Mozilla Firefox
- Microsoft Edge

Step 3: Key Differences.

Feature	Web Server	Web Browser
<i>Role</i>	<i>Provides content</i>	<i>Displays content</i>
<i>Type</i>	<i>Server – side software</i>	<i>Client – side application</i>
<i>Function</i>	<i>Stores websites</i>	<i>Accesses websites</i>
<i>Examples</i>	<i>Apache, Nginx</i>	<i>Chrome, Firefox</i>

Conclusion:

A web server hosts and delivers website data, while a web browser retrieves and displays that data to users, forming the foundation of web communication.

Quick Tip

Server = Sends web pages, Browser = Shows web pages.

2. Explain the purpose of protocols such as HTTP, HTTPS, FTP, and SMTP.

Correct Answer: These protocols define rules for communication over the internet: HTTP/HTTPS for web transfer, FTP for file transfer, and SMTP for sending emails.

Solution: Concept: Protocols are standardized rules that allow devices to communicate over networks. Different protocols serve different purposes depending on the type of data transfer.

Step 1: HTTP (HyperText Transfer Protocol).

- Used for transferring web pages on the internet.
- Works between web browsers and web servers.
- Not encrypted (less secure).

Example: Loading a basic webpage.

Step 2: HTTPS (HyperText Transfer Protocol Secure).

- Secure version of HTTP.
- Uses encryption (SSL/TLS).

- Protects data like passwords and banking details.

Example: Online shopping, banking websites.

Step 3: **FTP (File Transfer Protocol).**

- Used for transferring files between computers.
- Commonly used for uploading website files to servers.
- Requires authentication (username/password).

Example: Uploading files using FileZilla.

Step 4: **SMTP (Simple Mail Transfer Protocol).**

- Used for sending emails over the internet.
- Works between email clients and mail servers.
- Often combined with POP3 or IMAP for receiving emails.

Example: Sending an email via Gmail.

Step 5: **Comparison.**

Protocol	Purpose	Usage
<i>HTTP</i>	<i>Webpagetransfer</i>	<i>Browsingwebsites</i>
<i>HTTPS</i>	<i>Securewebtransfer</i>	<i>Onlinetransactions</i>
<i>FTP</i>	<i>Filetransfer</i>	<i>Upload/downloadfiles</i>
<i>SMTP</i>	<i>Emailsending</i>	<i>Sendingemails</i>

Conclusion:

HTTP and HTTPS enable web communication, FTP handles file transfers, and SMTP manages email sending, making them essential internet communication protocols.

Quick Tip

HTTP = Web, HTTPS = Secure Web, FTP = Files, SMTP = Send Mail.

3. Define Cloud Computing and provide two examples.

Correct Answer: Cloud computing is the delivery of computing services over the internet, allowing users to access storage, software, and resources without local hardware.

Solution: Concept: Cloud computing refers to using internet-based services instead of relying on local computers or servers. It provides on-demand access to computing resources such as storage, applications, and processing power.

Step 1: Definition of Cloud Computing.

Cloud computing is a technology that:

- Delivers computing services over the internet.

- Eliminates the need for local storage or infrastructure.
- Allows access anytime and anywhere.

Step 2: Key features.

- On-demand access
- Scalability
- Cost efficiency (pay-as-you-use)
- Remote accessibility

Step 3: Examples of Cloud Computing.

- **Google Drive:** Online storage for files and documents.
- **Microsoft OneDrive:** Cloud storage and file sharing.

Other examples (optional):

- Amazon Web Services (AWS)
- Dropbox
- Google Docs

Conclusion:

Cloud computing enables users to access computing resources via the internet, offering flexibility and scalability, with examples like Google Drive and OneDrive.

Quick Tip

Cloud = Store and access data online instead of your computer.

4. Differentiate between a Web Address (URL) and an Email Address with examples.

Correct Answer: A URL identifies the location of a resource on the web, while an email address identifies a user for sending and receiving electronic mail.

Solution: Concept: Both web addresses and email addresses are used on the internet but serve different purposes:

- URL → Access websites
- Email Address → Send and receive emails

Step 1: Web Address (URL).

- URL stands for **Uniform Resource Locator**.
- Identifies the location of a webpage or resource on the internet.
- Used in web browsers to access websites.

Example:

- https://www.google.com
- https://www.wikipedia.org

Step 2: Email Address.

- Used to **identify a user** in email communication.
- Required for sending and receiving electronic messages.
- Unique for each user.

Format:

username@domain.com

Example:

- example@gmail.com
- info@company.com

Step 3: Key Differences.

Feature	URL	Email Address
<i>Purpose</i>	<i>Access websites</i>	<i>Send/receive emails</i>
<i>Full form</i>	<i>Uniform Resource Locator</i>	<i>Electronic mail address</i>
<i>Used in</i>	<i>Web browsers</i>	<i>Email services</i>
<i>Format</i>	<i>Protocol + domain</i>	<i>username@domain</i>

Conclusion:

A URL is used to locate and access resources on the web, whereas an email address uniquely identifies a user for electronic communication.

Quick Tip

URL opens websites, Email connects people.

5. What is the role of a Search Engine, and how does it differ from a Web Portal?

Correct Answer: A search engine helps users find information on the internet, while a web portal provides a gateway to a collection of related services and resources.

Solution: Concept: Both search engines and web portals help users navigate the internet, but they serve different purposes and functionalities.

Step 1: Search Engine.

- A tool used to **search information on the internet**.
- Uses keywords to find relevant web pages.
- Indexes billions of web pages.
- Displays results as links ranked by relevance.

Examples:

- Google
- Bing
- Yahoo Search

Step 2: Web Portal.

- A **gateway website** that provides access to multiple services in one place.
- Offers organized information and tools.
- May require login for personalized services.

Services provided:

- Email
- News
- Weather updates
- Online services (banking, education portals)

Examples:

- Yahoo Portal
- Government portals (e.g., national service portals)
- Educational portals

Step 3: Key Differences.

Feature	Search Engine	Web Portal
<i>Purpose</i>	<i>Search information</i>	<i>Provide multiple services</i>
<i>Function</i>	<i>Finds web pages</i>	<i>Acts as service hub</i>
<i>Content</i>	<i>Links to external sites</i>	<i>Aggregated resources</i>
<i>Personalization</i>	<i>Minimal</i>	<i>Often personalized</i>

Conclusion:

A search engine helps users locate information across the web, while a web portal serves as a centralized platform offering a variety of integrated services and resources.

Quick Tip

Search Engine = Find information, Web Portal = Access many services in one place.

6. Define Plagiarism and list two ways a student can avoid it while using internet resources.

Correct Answer: Plagiarism is presenting someone else's work as your own; it can be avoided by proper citation and writing in your own words.

Solution: Concept: Plagiarism is an ethical issue related to academic honesty and intellectual property. It commonly occurs when using internet resources without proper acknowledgment.

Step 1: Definition of Plagiarism.

Plagiarism is:

- Copying someone else's work, ideas, or content
- Presenting it as your own without giving credit

It can include text, images, code, or research ideas.

Step 2: Why plagiarism is wrong.

- Violates academic integrity
- Disrespects original creators
- Can lead to penalties or loss of credibility

Step 3: Ways to avoid plagiarism.

1. Proper Citation:

- Always give credit to the original author.
- Mention sources using references, footnotes, or links.

2. Paraphrasing in Your Own Words:

- Rewrite information using your understanding.
- Avoid copying sentences directly.

Other ways (optional):

- Use quotation marks for direct quotes
- Use plagiarism detection tools
- Maintain a reference list

Conclusion:

Plagiarism is the act of using someone else's work without credit, and it can be avoided by proper citation and expressing ideas in your own words.

Quick Tip

If you didn't write it, cite it — the golden rule to avoid plagiarism.

7. List four essential Netiquettes every "netizen" should follow.

Correct Answer: Important netiquettes include being respectful online, protecting privacy, avoiding spam, and using appropriate language.

Solution: Concept: Netiquette (Internet etiquette) refers to the set of rules and guidelines for polite and responsible behavior online. It helps maintain a safe and respectful digital environment.

Step 1: Be Respectful and Polite.

- Treat others with respect in online communication.
- Avoid abusive language or cyberbullying.

Step 2: Protect Privacy.

- Do not share personal information unnecessarily.
- Respect others' privacy and confidentiality.

Step 3: Avoid Spamming.

- Do not send unwanted messages or advertisements.
- Share relevant and meaningful content only.

Step 4: Use Appropriate Language.

- Maintain professionalism in emails and posts.
- Avoid offensive or inappropriate words.

Other good practices (optional):

- Give credit to original creators
- Follow platform rules
- Think before posting

Conclusion:

Following netiquettes such as being respectful, protecting privacy, avoiding spam, and using appropriate language ensures responsible and positive online interactions.

Quick Tip

Think before you click — respect, responsibility, and privacy define good netiquette.

8. Explain Phishing and suggest two precautions to take during E-commerce transactions.

Correct Answer: Phishing is a cyberattack that tricks users into revealing sensitive information; precautions include verifying website authenticity and avoiding suspicious links.

Solution: Concept: Phishing is a common cybercrime where attackers impersonate trusted entities to steal personal or financial information, especially during online transactions.

Step 1: Definition of Phishing.

Phishing is a type of online fraud in which:

- Fake emails, messages, or websites are used
- To trick users into revealing passwords, OTPs, or card details

Examples:

- Fake bank emails asking for login credentials
- Fraudulent shopping websites offering unrealistic discounts

Step 2: Why phishing is dangerous.

- Financial loss
- Identity theft
- Unauthorized account access

Step 3: Precautions during E-commerce transactions.

1. Verify Website Authenticity:

- Check for HTTPS and padlock symbol in the address bar.
- Buy only from trusted and well-known websites.

2. Avoid Suspicious Links:

- Do not click on unknown email or SMS links.
- Type the website URL manually when shopping online.

Other precautions (optional):

- Use secure payment methods
- Enable two-factor authentication
- Do not share OTPs with anyone

Conclusion:

Phishing is a deceptive cyberattack aimed at stealing sensitive information, and it can be prevented during e-commerce transactions by verifying secure websites and avoiding suspicious links.

Quick Tip

If an online deal looks too good to be true, it probably is — always verify before you buy.
