

CBSE Class 10 Computer Applications Question Paper 2026 with Solutions

Time Allowed :2 Hour	Maximum Marks :50	Total Questions :21
----------------------	-------------------	---------------------

General Instructions

Read the following instructions very carefully and strictly follow them:

1. Please read the instructions carefully.
2. This question paper consists of 21 questions in two Sections : Section A and Section B.
3. Section A has Objective type questions, whereas Section B contains Subjective type questions.
4. Out of the given $(5 + 16) = 21$ questions, a candidate has to answer $(5 + 10) = 15$ questions in the allotted (maximum) time of 2 hours.
5. All questions of a particular section must be attempted in the correct order.
6. Section A : Objective Type Questions (24 marks) :
 - (a) This section has 5 questions.
 - (b) There is no negative marking.
 - (c) Do as per the instructions given.
 - (d) Marks allotted are mentioned against each question/part.
7. Section B : Subjective Type Questions (26 marks) :
 - (a) This section has 16 questions.
 - (b) A candidate has to do 10 questions.
 - (c) Do as per the instructions given.
 - (d) Marks allotted are mentioned against each question/part.

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:

Step 1: Understanding the Question.

The question asks to differentiate between a web server and a web browser, which are the two primary components of the client-server architecture that powers the World Wide Web.

Step 2: Detailed Explanation of a Web Server.

A **Web Server** is a powerful computer or software that **stores** website files (like HTML, CSS,

images) and **delivers** them to users upon request.

- **Role:** It acts as the host for websites. When you type a web address, your browser sends a request to the server, and the server sends back the webpage data.
- **Function:** It processes incoming requests via protocols like HTTP/HTTPS and serves the requested content.
- **Examples:** Popular web server software includes Apache HTTP Server, Nginx, and Microsoft Internet Information Services (IIS).

Step 3: Detailed Explanation of a Web Browser.

A **Web Browser** is a software application installed on a user's device (like a computer or smartphone) used to **access** and **display** information from the World Wide Web.

- **Role:** It acts as the client that requests information from the server.
- **Function:** It sends requests to web servers, receives the response (data), and renders it into a human-readable webpage. It interprets languages like HTML, CSS, and JavaScript.
- **Examples:** Common web browsers are Google Chrome, Mozilla Firefox, Microsoft Edge, and Safari.

Step 4: Key Differences Summarized.

Feature	Web Server	Web Browser
Primary Role	To serve/provide content.	To request/display content.
System Type	It is server-side software.	It is a client-side application.
Main Function	Hosts and delivers websites.	Accesses and renders websites.
Interaction	Responds to requests.	Initiates requests.

Step 5: Final Answer.

In essence, a web server is the backend system that stores and sends website data, while a web browser is the frontend application that a user interacts with to request and view that data. They work together to make the internet accessible.

💡 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:

Step 1: Understanding the Question.

The question asks for an explanation of the purpose of four fundamental internet protocols: HTTP, HTTPS, FTP, and SMTP. Protocols are the standardized sets of rules that govern data communication over a network.

Step 2: Detailed Explanation of Each Protocol.

1. HTTP (HyperText Transfer Protocol):

- **Purpose:** It is the foundation of data communication for the World Wide Web. Its primary function is to transfer hypertext (i.e., web pages) from a web server to a web browser.
- **Security:** It is an unencrypted protocol, meaning the data transferred can be intercepted and read.

2. HTTPS (HyperText Transfer Protocol Secure):

- **Purpose:** It is the secure version of HTTP. It performs the same function of transferring web data but adds a layer of security.
- **Security:** It uses encryption (SSL/TLS) to secure the connection between the browser and the server, protecting sensitive data like passwords, credit card numbers, and personal information. You can identify it by the padlock icon in the browser's address bar.

3. FTP (File Transfer Protocol):

- **Purpose:** This protocol is specifically designed for transferring computer files from one host to another over a TCP-based network, such as the internet.
- **Usage:** It is commonly used by web developers to upload website files to a server.

4. SMTP (Simple Mail Transfer Protocol):

- **Purpose:** This is the standard protocol for sending electronic mail (email) from an email client to an email server, and between email servers.

- **Usage:** When you click "Send" on an email, SMTP is the protocol that handles its delivery across the internet. It is used for outgoing mail.

Step 3: Final Answer.

In summary, these protocols each serve a distinct and vital role in internet communication: HTTP for standard web browsing, HTTPS for secure web browsing, FTP for transferring files, and SMTP for sending emails.

💡 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:

Step 1: Understanding the Question.

The question asks for a definition of "Cloud Computing" and two practical examples of cloud services.

Step 2: Defining Cloud Computing.

Cloud computing is the on-demand delivery of computing services—including servers, storage, databases, networking, software, and analytics—over the Internet ("the cloud").

Instead of owning and maintaining your own computing infrastructure, you can access these services from a cloud provider. This allows you to pay only for what you use and access your data and applications from any device with an internet connection.

Step 3: Key Characteristics.

- **On-Demand Self-Service:** Users can access computing resources as needed without human intervention.
- **Broad Network Access:** Services are available over the network and accessed through standard mechanisms (e.g., web browsers).
- **Resource Pooling:** The provider's resources are pooled to serve multiple consumers.
- **Scalability:** Resources can be rapidly scaled up or down to meet demand.

Step 4: Providing Two Examples.

Here are two common examples of cloud computing services:

1. Google Drive:

- This is a cloud storage service where users can store files (documents, photos, videos) online.
- The files are not stored on the user's local device but on Google's servers, and can be accessed from anywhere with an internet connection. It also allows for collaboration through services like Google Docs and Sheets.

2. Netflix:

- This is a streaming service that uses cloud computing to store its vast library of movies and TV shows.
- When you stream a video, you are accessing data from Netflix's cloud servers (which run on Amazon Web Services - AWS), not downloading the entire file to your device.

Step 5: Final Answer.

In conclusion, cloud computing provides computing services over the internet, removing the need for local hardware. Services like Google Drive (for storage) and Netflix (for media streaming) are prime examples of how we use the cloud in our daily lives.

💡 Quick Tip

Cloud = Store and access data online instead of on 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:

Step 1: Understanding the Question.

The question asks for the differences between a web address (URL) and an email address, including their purpose and structure, supported by examples.

Step 2: Explaining a Web Address (URL).

A **Web Address**, or **URL (Uniform Resource Locator)**, is a reference to a web resource

that specifies its location on a computer network.

- **Purpose:** Its primary function is to locate and allow access to a specific resource on the internet, such as a webpage, image, or document.
- **Structure:** It typically consists of a protocol (like 'https://'), a domain name (like 'www.example.com'), and sometimes a path to a specific file or page (like '/about-us.html').
- **Example:** 'https://www.wikipedia.org' points to the homepage of the Wikipedia website.

Step 3: Explaining an Email Address.

An **Email Address** is a unique identifier for an electronic mailbox.

- **Purpose:** It is used to send and receive electronic mail (emails). It directs messages to a specific user's account on a mail server.
- **Structure:** It has a specific format: 'local-part@domain'. The part before the '@' symbol is the username, and the part after is the domain name of the email service provider.
- **Example:** 'john.doe@gmail.com' directs an email to the user "john.doe" whose mailbox is hosted on the "gmail.com" domain.

Step 4: Key Differences Summarized.

Feature	Web Address (URL)	Email Address
Purpose	To locate a web resource.	To identify a user's mailbox.
Usage	Used in a web browser.	Used in an email client.
Action	Accessing/retrieving information.	Sending/receiving messages.
Key Symbol	Uses '://' and '/'.	Uses the '@' symbol.

Step 5: Final Answer.

The fundamental difference is their purpose: a URL is an address for a resource on the web, while an email address is an address for a person's digital mailbox. One is for finding places/things online, the other is for communicating with people.

💡 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:

Step 1: Understanding the Question.

The question asks to define the role of a search engine and explain how it is different from a web portal.

Step 2: Role and Function of a Search Engine.

A **Search Engine** is a software system designed to carry out web searches. It scours the internet in a systematic way for particular information specified in a textual web search query.

- **Core Role:** To help users find specific information scattered across the vast World Wide Web.
- **How it works:** It uses automated programs called "crawlers" or "spiders" to index billions of webpages. When a user enters a keyword, the search engine's algorithm sifts through this index to provide a ranked list of the most relevant results.
- **Examples:** Google, Bing, DuckDuckGo.

Step 3: Role and Function of a Web Portal.

A **Web Portal** is a specially designed website that brings information from diverse sources together in a uniform way. It serves as a single point of access to information, services, and applications.

- **Core Role:** To act as a "gateway" or a starting point for users, offering a collection of services and curated content.
- **Features:** Portals are often personalized and may require a login. They typically offer services like email, news headlines, weather forecasts, stock quotes, and links to other websites.
- **Examples:** University portals (for students to access courses and grades), government portals, and early internet services like Yahoo!.

Step 4: Key Differences.

- **Focus:** A search engine's focus is broad—to find information across the entire web. A web portal's focus is narrow—to provide a curated set of services and information in one place.

- **Content:** A search engine primarily displays links to external content. A web portal displays its own aggregated content and services.
- **Interaction:** Users go to a search engine to leave and find other sites. Users go to a web portal to stay and use its integrated services.

Step 5: Final Answer.

In short, a search engine is a tool for discovery across the open web, while a web portal is a centralized destination offering a bundle of services. Think of a search engine as a map to find any address, and a web portal as a shopping mall with many different stores inside one building.

💡 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:

Step 1: Understanding the Question.

This question has two parts: first, to define the term "plagiarism," and second, to provide two effective methods for a student to avoid it, especially when using online resources.

Step 2: Defining Plagiarism.

Plagiarism is the act of taking someone else's work, ideas, or words and presenting them as one's own without giving proper credit to the original source. It is a form of intellectual theft and a serious breach of academic and ethical standards. It is not limited to text; it can also include images, data, code, and other creative works.

Step 3: Two Methods to Avoid Plagiarism.

Here are two essential practices for students to maintain academic integrity:

Method 1: Citing Sources Properly.

- **What it is:** Citation is the practice of acknowledging the sources of information you have used in your work. Whenever you use a direct quote, a statistic, an idea, or any information that is not common knowledge, you must indicate where it came from.

- **How to do it:** This can be done through footnotes, endnotes, or a bibliography/works cited page, following a specific citation style (like APA, MLA, etc.). This gives credit to the original author and allows readers to find the source themselves.

Method 2: Paraphrasing and Summarizing.

- **What it is:** Instead of copying text word-for-word, you should process the information and express it in your own words. Paraphrasing involves restating a specific passage in a different way, while summarizing involves condensing the main ideas of a source into a shorter form.
- **How to do it:** Read the source material, understand its meaning, and then write it out in your unique style and sentence structure. Even when you paraphrase or summarize, you must still cite the original source.

Step 4: Final Answer.

Plagiarism is the unethical act of using another's work without attribution. Students can avoid it by diligently **citing** every source they use and by **paraphrasing** or summarizing information in their own words rather than copying it directly.

💡 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:

Step 1: Understanding the Question.

The question asks for four essential rules of "Netiquette" that every internet user (or "netizen") should follow to ensure positive and safe online interactions. Netiquette is a combination of the words "network" and "etiquette."

Step 2: Detailed Explanation of Four Netiquettes.

Here are four fundamental principles of good netiquette:

1. Be Respectful and Courteous:

- Treat others online as you would want to be treated in real life. Avoid personal attacks, abusive language, name-calling, and cyberbullying. Remember that there is a real person with feelings behind every screen. Engage in constructive discussions, even when you disagree.

2. Protect Your Own and Others' Privacy:

- Do not share sensitive personal information (like your address, phone number, or passwords) online. Equally important, do not share someone else's private information without their explicit permission. Respecting privacy is a cornerstone of online safety and trust.

3. Do Not Spam:

- Spamming refers to sending unsolicited, irrelevant, or repetitive messages to a large number of recipients. This includes chain letters, fraudulent messages, and excessive advertising. It clutters communication channels and is generally considered intrusive and annoying. Share content that is relevant and adds value to the conversation.

4. Fact-Check Before Sharing:

- The internet allows misinformation and fake news to spread rapidly. Before you share an article, image, or piece of news, take a moment to verify its authenticity from reliable sources. Spreading false information, even unintentionally, can have harmful consequences. Be a responsible digital citizen.

Step 3: Final Answer.

Four essential netiquettes for every netizen are: to be respectful and courteous in all communications, to protect personal privacy, to avoid spamming, and to fact-check information before sharing. These practices contribute to a healthier and more reliable digital environment.

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:

Step 1: Understanding the Question.

The question consists of two parts: first, to define "Phishing," and second, to suggest two specific safety measures to protect oneself during online shopping (e-commerce transactions).

Step 2: Defining Phishing.

Phishing is a type of cybercrime where attackers attempt to trick individuals into revealing sensitive personal information, such as usernames, passwords, credit card details, or bank account numbers. They do this by impersonating a trustworthy entity (like a bank, a popular e-commerce site, or a government agency) in an electronic communication, typically an email, SMS, or a fake website. The goal is to use this stolen information for fraudulent purposes, such as identity theft or financial loss.

Step 3: Two Precautions for E-commerce Transactions.

To stay safe while shopping online, here are two crucial precautions:

1. Verify the Website's Security and Authenticity:

- Always check the website's address bar before entering any payment information. A secure website will use **HTTPS** (not just HTTP), and you should see a **padlock icon**. This indicates that the connection between your browser and the website is encrypted.
- Be wary of websites with misspelled domain names (e.g., 'amaz0n.com' instead of 'amazon.com'), as this is a common tactic used in phishing. Stick to well-known and reputable retailers.

2. Use Secure Payment Methods and Avoid Public Wi-Fi:

- When possible, use secure payment options like credit cards (which often offer better fraud protection than debit cards) or trusted third-party payment services like PayPal. Avoid making direct bank transfers to unknown sellers.
- Never conduct financial transactions while connected to public or unsecured Wi-Fi networks (like those in cafes or airports). These networks are vulnerable, and hackers can potentially intercept your data. Always use a secure, private network for online shopping.

Step 4: Final Answer.

Phishing is a cyberattack using deception to steal sensitive data. To protect against it during e-commerce transactions, one must always verify that the website is secure (using HTTPS) and use safe payment methods on a private network, avoiding suspicious links and offers.

 Quick Tip

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