# Topic: The differences between the internet and the World Wide Web (WWW)

Reading Time: 15 mins

## Note\* Highlight important/core points while reading

* Read the content and write the answers given in the document in your words, to get the solid grip on topic.

### Differences Between the Internet and the World Wide Web (WWW)

The **Internet** and the **World** **Wide** **Web** **(WWW)** are closely related but distinct concepts.

|  |  |  |
| --- | --- | --- |
| **Feature** | **Internet** | **World** **Wide** **Web** **(WWW)** |
| **Definition** | A global network of interconnected | A system of interlinked web pages and |
|  | computers that communicate using | resources accessed via the Internet |
|  | protocols like TCP/IP. | using web browsers. |
| **Function** | Provides the infrastructure for | Uses the Internet to access and display |
|  | communication, data transfer, and | web pages, multimedia, and |
|  | networking. | hyperlinked documents. |
| **Components** | Includes servers, routers, cables, data | Consists of websites, web pages, |
|  | centers, and protocols (TCP/IP, DNS, | hyperlinks, and web technologies |
|  | etc.). | (HTML, CSS, JavaScript). |
| **Protocols** | Uses TCP/IP (Transmission Control | Uses HTTP (Hypertext Transfer |
| **Used** | Protocol/Internet Protocol), FTP, | Protocol) and HTTPS for secure |
|  | SMTP, etc. | communication. |
| **Example** | Email, file transfer, video | Websites, blogs, e-commerce, social |
| **Services** | conferencing, online gaming. | media platforms. |

## How They Work

### The Internet's Working Mechanism

* + The Internet is a global network of computers connected through fiber-optic cables, satellites, and wireless technologies.
  + It uses the **TCP/IP** **protocol** **suite** to facilitate communication.
  + Devices on the Internet are identified by **IP** **addresses** and domain names (e.g., google.com).
  + Data is transmitted in the form of **packets** that travel through routers and servers to reach their destination.

### The World Wide Web's Working Mechanism

* + The WWW is an application that runs on the Internet.
  + Websites are hosted on **web** **servers**, which store web pages written in **HTML,** **CSS,** **and** **JavaScript**.
  + Users access the WWW using **web** **browsers** (such as Chrome, Firefox, or Edge).
  + Web pages are connected through **hyperlinks** and can include multimedia elements like text, images, and videos.
  + When a user enters a **URL** **(Uniform** **Resource** **Locator)** in a browser, the **DNS** **(Domain** **Name** **System)** translates it into an IP address, allowing the browser to request the webpage from the corresponding web server.
  + The webpage is then sent back to the user’s device using **HTTP** **or** **HTTPS** **protocols** and displayed in the browser.

## A-Rated Questions/Answers By Examiner

### Q1: Define the Internet and the World Wide Web (WWW). Answer:

* + The **Internet** is a global network of interconnected computers that communicate using the **TCP/IP** **protocol**.
  + The **World** **Wide** **Web** **(WWW)** is a collection of **interlinked** **web** **pages** **and** **resources** accessed via the Internet using web browsers.

### Q2: Explain two differences between the Internet and the [WWW](http://www/).

**Answer:**

1. **The** **Internet** is the physical infrastructure that allows communication, whereas **the** **WWW** is an application that provides access to web pages.
2. **The** **Internet** uses multiple protocols such as TCP/IP and FTP, while **the** **WWW** mainly relies on HTTP/HTTPS.

### Q3: What is the role of a web browser in accessing the World Wide Web?

**Answer:** A web browser is a software application that retrieves, interprets, and displays web pages from the [WWW](http://www/). It sends requests to web servers using the **HTTP/HTTPS** **protocols** and presents web content (HTML, images, videos, and interactive elements) to users.

**Q4:** **How** **does** **a** **DNS** **(Domain** **Name** **System)** **work** **when** **accessing** **a** **website?** **Answer:** When a user enters a URL (e.g., [www.example.com](http://www.example.com/)) into a web browser:

1. The browser requests the **IP** **address** of the website from a **DNS** **server**.
2. The DNS translates the domain name into an IP address.
3. The browser uses the IP address to request the web page from the web server.
4. The web server responds with the web page data, which is displayed in the browser.

### Q5: What is the purpose of the HTTP and HTTPS protocols in web communication?

**Answer:**

* + **HTTP** **(Hypertext** **Transfer** **Protocol)** is used to transfer web pages and resources between a web server and a browser.
  + **HTTPS** **(Hypertext** **Transfer** **Protocol** **Secure)** is an encrypted version of HTTP that ensures secure communication using **SSL/TLS** **encryption** to protect user data from cyber threats.

## Write your Answers on your Notebook and Verify it on Next Screen

**Q6:** **How** **does** **data** **travel** **across** **the** **Internet** **to** **reach** **its** **destination?**

**Q7:** **What** **are** **some** **examples** **of** **services** **provided** **by** **the** **Internet** **that** **are** **not** **part** **of** **the** **World** **Wide** **Web?**

**Q8:** **Why** **is** **the** **Internet** **considered** **the** **backbone** **of** **the** **World** **Wide** **Web?**

**Q9:** **What** **role** **do** **web** **servers** **play** **in** **the** **functioning** **of** **the** **World** **Wide** **Web?**

**Q10:** **How** **does** **a** **URL** **(Uniform** **Resource** **Locator)** **help** **users** **navigate** **the** **World** **Wide** **Web?**

1. **Answer:**
   1. Data is broken into packets before being sent across the Internet.
   2. Packets travel through various routers and servers using the best available path.
   3. The destination device reassembles the packets to retrieve the original data.
   4. This process is governed by the TCP/IP protocol to ensure reliable communication.

### Answer:

* 1. Email services (e.g., Gmail, Outlook) use protocols like SMTP, IMAP, and POP3.
  2. File transfer services via FTP (File Transfer Protocol).
  3. Video conferencing applications like Zoom and Microsoft Teams.
  4. Online gaming and streaming services like Netflix and Xbox Live.

### Answer:

* 1. The WWW relies on the Internet to transmit data between users and web servers.
  2. Without the Internet’s infrastructure (cables, servers, and networking protocols), web pages and online services could not function.
  3. The Internet enables global connectivity, allowing web browsers to access and display web pages.

### Answer:

* 1. Web servers store and host websites, making web pages accessible to users.
  2. When a browser requests a web page, the web server processes the request and sends the required files (HTML, CSS, JavaScript) to the browser.
  3. Web servers use HTTP/HTTPS to facilitate secure communication between clients and websites.

### Answer:

* 1. A URL is a unique address used to locate resources on the [WWW](http://www/).
  2. It consists of different parts, including the protocol (HTTP/HTTPS), domain name (e.g., google.com), and file path (e.g., /index.html).
  3. The URL directs the browser to the correct web server and retrieves the requested webpage.

# Topic: Uniform resource locators (URLs)

Reading Time: 15 mins

## Note\* Highlight important/core points while reading

* + - Read the content and write the answers given in the document in your words, to get the solid grip on topic.

### Uniform Resource Locators (URLs)

A **Uniform** **Resource** **Locator** **(URL)** is the address used to access resources (such as web pages) on the World Wide Web (WWW). It provides the necessary information for a web browser to locate and retrieve a web resource.

### Structure of a URL

A typical URL consists of multiple components: https://[www.example.com/section/page.html](http://www.example.com/section/page.html)

1. **Protocol** **(Scheme)** → http:// or https://
   * Defines the communication rules between the web browser and the server.
   * **HTTP** **(Hypertext** **Transfer** **Protocol)** is used for standard web pages.
   * **HTTPS** **(Hypertext** **Transfer** **Protocol** **Secure)** provides secure communication using encryption (SSL/TLS).
2. **Domain** **Host** **(Subdomain)** → [www.](http://www/)
   * This is an optional part of the URL.
   * www (World Wide Web) is a common subdomain, but other subdomains like mail. (for emails) or blog. (for blogs) can also be used.
3. **Domain** **Name** → example
   * The unique name of the website, chosen by the owner.
   * Example: google, facebook, bbc, wikipedia.
4. **Domain** **Type** **(Top-Level** **Domain** **-** **TLD)** → .com

* Indicates the type or purpose of the website.
* Common domain types include:
  + .com → Commercial websites
  + .org → Organizations (non-profits, charities)
  + .net → Networking-related sites
  + .gov → Government sites
  + .edu → Educational institutions

1. **Country** **Code** **(Optional** **-** **ccTLD)** → .uk

* Specifies the country where the website is registered.
* Examples:
  + .uk → United Kingdom
  + .de → Germany
  + .cy → Cyprus

1. **Path** **(Optional)** → /section/page.html

* Specifies the exact location of a page or resource within the website.
* Example: /products/shoes.html leads to a specific product page.

### How a URL Works

1. The user enters a URL into the web browser.
2. The browser sends a request using the protocol (http or https).
3. The **Domain** **Name** **System** **(DNS)** translates the domain name into an **IP** **address**.
4. The browser connects to the web server at that IP address.
5. The server locates the requested resource (web page, file, etc.) and sends it to the browser.
6. The browser renders the web page for the user to view.

## A-Rated Questions/Answers By Examiner

**Q1:** **What** **is** **a** **URL,** **and** **why** **is** **it** **important?**

**Answer:** A **Uniform** **Resource** **Locator** **(URL)** is the web address used to access websites and online resources. It is important because it provides the exact location of a resource on the **World** **Wide** **Web** **(WWW)**, allowing users and browsers to retrieve web pages efficiently.

### Q2: Name and explain the main components of a URL.

**Answer:**

1. **Protocol** → Specifies how data is transferred (e.g., http://, https://).
2. **Domain** **Host** → Identifies the subdomain (e.g., www.).
3. **Domain** **Name** → Represents the website's name (e.g., example).
4. **Domain** **Type** **(TLD)** → Indicates the type of website (e.g., .com, .org).
5. **Country** **Code** **(ccTLD** **-** **Optional)** → Shows the country of registration (e.g., .uk,

.de).

1. **Path** **(Optional)** → Defines the specific webpage or resource being accessed (e.g.,

/contact.html).

### Q3: What is the difference between HTTP and HTTPS? Answer:

* + **HTTP** **(Hypertext** **Transfer** **Protocol)** transmits data without encryption. It is less secure and can be intercepted.
  + **HTTPS** **(Hypertext** **Transfer** **Protocol** **Secure)** encrypts data using **SSL/TLS** **encryption**, making it more secure and protecting user data from cyber threats.

### Q4: What is a domain name, and how is it different from an IP address? Answer:

* + A **domain** **name** (e.g., google.com) is a human-friendly address used to access websites.
  + An **IP** **address** (e.g., 192.168.1.1) is a numerical address assigned to devices on the Internet.
  + The **Domain** **Name** **System** **(DNS)** translates domain names into IP addresses, allowing users to access websites without remembering numerical IP addresses.

**Q5:** **What** **is** **the** **purpose** **of** **a** **country** **code** **in** **a** **URL?**

**Answer:** A **country** **code** **top-level** **domain** **(ccTLD)** (e.g., .uk, .in, .fr) indicates the country where a website is registered or primarily serves. It helps users identify the geographic origin of a website.

## Write your Answers on your Notebook and Verify it on Next Screen

**Q6:** **How** **does** **the** **Domain** **Name** **System** **(DNS)** **help** **in** **accessing** **a** **website** **using** **a** **URL?**

**Q7:** **Why** **is** **HTTPS** **preferred** **over** **HTTP** **for** **modern** **websites?**

**Q8:** **What** **is** **a** **subdomain,** **and** **how** **does** **it** **differ** **from** **a** **main** **domain?**

**Q9:** **How** **does** **a** **URL** **help** **in** **SEO** **(Search** **Engine** **Optimization)?**

**Q10:** **What** **is** **a** **query** **string** **in** **a** **URL,** **and** **how** **is** **it** **used?**

### Answer:

* 1. When a user enters a URL, the browser queries a DNS server to resolve the domain name into an IP address.
  2. The DNS system searches for the corresponding IP address of the domain name entered.
  3. Once the IP address is found, the browser establishes a connection with the web server.
  4. The server then sends back the requested webpage, which is displayed in the browser.

### Answer:

* 1. HTTPS encrypts data using SSL/TLS, ensuring secure communication between the browser and the web server.
  2. It protects sensitive information such as login credentials, payment details, and personal data from cyber threats.
  3. HTTPS improves trustworthiness, as browsers label HTTP sites as "Not Secure."
  4. Search engines like Google prioritize HTTPS websites in search rankings.

### Answer:

* 1. A subdomain is a prefix added before the main domain to categorize different sections of a website (e.g., blog.example.com).
  2. It acts as a separate website under the same domain name but can serve a different purpose.
  3. Main domains (e.g., example.com) are the central identifiers of a website, while subdomains help organize content.
  4. Examples:
     + **mail.google.com** (Gmail service)
     + **news.bbc.com** (BBC news section)

### Answer:

* 1. A well-structured URL improves a website's visibility in search engines.
  2. Using keywords in the URL (e.g., **example.com/best-laptops-2024**) increases relevance.
  3. Short and descriptive URLs improve user experience and click-through rates.
  4. HTTPS URLs contribute to better search rankings as they indicate a secure website.

### Answer:

* 1. A query string is a part of a URL that contains parameters, typically used to pass information to web applications.
  2. It starts with a ? and consists of key-value pairs separated by &.
  3. Example: https:/[/www.example.com/search?q=laptops&category=electronics](http://www.example.com/search?q=laptops&category=electronics)
  4. Query strings are commonly used in search results, tracking, and dynamic content generation.

# Topic: HTTP and HTTPS

Reading Time: 15 mins

## Note\* Highlight important/core points while reading

* Read the content and write the answers given in the document in your words, to get the solid grip on topic.

### HTTP and HTTPS

HTTP (**Hypertext** **Transfer** **Protocol**) and HTTPS (**Hypertext** **Transfer** **Protocol** **Secure**) are the two main protocols used for communication between web browsers and web servers on

the **World** **Wide** **Web** **(WWW)**.

### HTTP (Hypertext Transfer Protocol) - Working Mechanism

HTTP is a **stateless** communication protocol used for transmitting web pages and other resources over the Internet. It follows a **request-response** **model**, meaning:

1. The user enters a URL in the web browser.
2. The browser sends an **HTTP** **request** to the web server.
3. The web server processes the request and sends back the requested web page as an **HTTP** **response**.
4. The browser receives the response and displays the web page to the user.

### Key Features of HTTP:

* + **Stateless** → Each request is independent, meaning the server does not remember previous

interactions.

* + **Unsecured** → Data is transmitted in **plain** **text**, making it vulnerable to hackers.
  + **Uses** **Port** **80** → Default port for HTTP communication.
  + **Faster** **than** **HTTPS** → Since it does not involve encryption.

### Example of an HTTP URL:

[http://www.example.com](http://www.example.com/)

### HTTPS (Hypertext Transfer Protocol Secure)

HTTPS is a **secure** version of HTTP that encrypts the data transmitted between the web browser and the web server using **SSL** **(Secure** **Sockets** **Layer)** **or** **TLS** **(Transport** **Layer**

**Security)** encryption.

### How HTTPS Works:

1. The user enters a URL that starts with https://.
2. The browser requests a **digital** **certificate** **(SSL/TLS** **certificate)** from the web server.
3. The web server provides the certificate, which contains a **public** **key** for encryption.
4. The browser verifies the certificate’s authenticity (issued by a **Certificate** **Authority** **(CA)**).
5. If the certificate is valid, an **encrypted** **connection** is established between the browser and the server.
6. The browser and server exchange encrypted data, ensuring **secure** **communication**.

### Key Features of HTTPS:

* + **Encrypted** **Communication** → Protects user data from hackers.
  + **Authentication** → Ensures that the website is genuine and not a fake/phishing site.
  + **Uses** **Port** **443** → Default port for HTTPS communication.
  + **Slightly** **Slower** **than** **HTTP** → Due to encryption processes.

**Example** **of** **an** **HTTPS** **URL:** [https://www.secure-website.com](https://www.secure-website.com/) **Differences** **Between** **HTTP** **and** **HTTPS**

|  |  |  |
| --- | --- | --- |
| **Feature** | **HTTP** | **HTTPS** |
| **Security** | Not secure | Secure (encrypted using SSL/TLS) |
| **Data** **Transmission** | In plain text | Encrypted |
| **Port** **Used** | 80 | 443 |
| **Speed** | Faster | Slightly slower due to encryption |
| **Authentication** | No authentication | Uses SSL/TLS certificate to verify identity |

**Usage** Used for non-sensitive data

Used for secure transactions like online banking, shopping, etc.

## A-Rated Questions/Answers By Examiner

**Q1:** **What** **is** **HTTP,** **and** **how** **does** **it** **work?**

**Answer:** HTTP (**Hypertext** **Transfer** **Protocol**) is a communication protocol used for transmitting web pages and resources over the Internet. It follows a **request-response** **model**, where:

1. A browser sends an **HTTP** **request** to a web server.
2. The web server processes the request and responds with the requested web page as an **HTTP** **response**.
3. The browser then displays the web page to the user.

**Q2:** **What** **is** **the** **main** **difference** **between** **HTTP** **and** **HTTPS?** **Answer:** The main difference is **security**:

* + **HTTP** sends data in plain text and is **not** **secure**.
  + **HTTPS** encrypts data using **SSL/TLS**, making it **secure** against cyber threats like hacking and eavesdropping.

**Q3:** **Why** **is** **HTTPS** **important** **for** **websites** **handling** **sensitive** **data?** **Answer:** HTTPS is important because it:

1. **Encrypts** **data** to protect user information (e.g., passwords, credit card details).
2. **Prevents** **hacking** **and** **eavesdropping** by securing communication.
3. **Provides** **authentication**, ensuring users interact with the genuine website and not a fake or phishing site.

**Q4:** **What** **is** **an** **SSL/TLS** **certificate,** **and** **what** **is** **its** **role** **in** **HTTPS?** **Answer:** An **SSL/TLS** **certificate** is a digital certificate issued by a **Certificate**

**Authority** **(CA)** to secure communication between web browsers and servers. It:

* + Provides **encryption** for secure data transfer.
  + **Authenticates** the identity of the website.
  + Prevents cyber-attacks such as **man-in-the-middle** **(MITM)** **attacks**.

### Q5: What are the default ports used for HTTP and HTTPS communication? Answer:

* + HTTP uses **Port** **80**.
  + HTTPS uses **Port** **443**.

## Write your Answers on your Notebook and Verify it on Next Screen

**Q6:** **How** **does** **HTTPS** **improve** **user** **trust** **and** **website** **credibility?**

**Q7:** **What** **is** **a** **Certificate** **Authority** **(CA),** **and** **why** **is** **it** **important** **in** **HTTPS?**

**Q8:** **What** **are** **some** **common** **cyber** **threats** **that** **HTTPS** **helps** **protect** **against?**

**Q9:** **Why** **is** **HTTP** **still** **used** **despite** **its** **security** **risks?**

**Q10:** **How** **can** **a** **website** **transition** **from** **HTTP** **to** **HTTPS?**

1. **Answer:**
   1. HTTPS displays a padlock icon in the browser address bar, indicating a secure connection.
   2. Websites with HTTPS are less likely to be flagged as "Not Secure" by browsers.
   3. Users feel more confident sharing personal and financial information on HTTPS- enabled sites.
   4. Search engines like Google prioritize HTTPS websites, improving their ranking in search results.

### Answer:

* 1. A Certificate Authority (CA) is an entity that issues SSL/TLS certificates to verify website authenticity.
  2. CAs ensure that the website is legitimate and not operated by hackers.
  3. Popular CAs include Let’s Encrypt, DigiCert, and GlobalSign.
  4. Browsers trust HTTPS websites only if their certificates are issued by a recognized CA.

### Answer:

* 1. **Man-in-the-Middle** **(MITM)** **Attacks** – Prevents attackers from intercepting and altering data.
  2. **Phishing** **Attacks** – Ensures users are connecting to legitimate websites, reducing fake site scams.
  3. **Data** **Eavesdropping** – Encrypts communication, preventing hackers from stealing sensitive information.
  4. **Data** **Tampering** – Ensures that data exchanged between the browser and server is not altered.

### Answer:

* 1. HTTP is faster since it does not require encryption, making it useful for non-sensitive content.
  2. Some legacy systems and internal networks still rely on HTTP.
  3. HTTPS requires an SSL/TLS certificate, which may be costly for some website owners.
  4. Websites that do not handle user data, such as informational blogs, may not prioritize HTTPS.

### Answer:

* 1. Obtain an SSL/TLS certificate from a trusted Certificate Authority (CA).
  2. Install and configure the certificate on the web server.
  3. Update internal links and ensure all resources (images, scripts) load over HTTPS.
  4. Redirect HTTP traffic to HTTPS using server settings (e.g., 301 redirects in

.htaccess).

* 1. Test and verify the HTTPS implementation to ensure security and performance.

# Topic: Web browsers

Reading Time: 15 mins

## Note\* Highlight important/core points while reading

* + - Read the content and write the answers given in the document in your words, to get the solid grip on topic.

### Web Browsers

A **web** **browser** is a software application used to access, retrieve, and display web pages and other online resources from the **World** **Wide** **Web** **(WWW)**. It allows users to navigate websites, interact with online content, and manage their browsing experience efficiently.

### Main Features of Web Browsers

1. **Home** **Page**
   * The **home** **page** is the first page that appears when the browser is opened.
   * Users can set their preferred home page (e.g., [www.google.com).](http://www.google.com/)

### Bookmarks (Favorites)

* + Browsers allow users to **save** **frequently** **visited** **web** **pages** as bookmarks.
  + This makes it easier to access favorite websites quickly without typing the URL.

### Browsing History

* + The browser stores a **record** **of** **visited** **websites** (user history).
  + Users can view and revisit previously accessed websites.

### Navigation Controls

* + Browsers provide **back** **and** **forward** **buttons** to move between previously opened web pages.
  + Users can **refresh** a web page to reload updated content.

### Multiple Tabs

* + Users can open **multiple** **web** **pages** in a single browser using **tabs**.
  + This allows efficient multitasking without opening separate windows.

### Cookies

* + Cookies are **small** **text** **files** stored on the user’s computer by websites.
  + They store user preferences, login sessions, and browsing data.
  + Example: A shopping website may use cookies to remember items in a cart.

### Hyperlinks and Navigation

* + Hyperlinks (or **links**) allow users to move between different web pages.
  + A hyperlink can be opened in two ways:
    - **Same** **tab** → Click the link normally.
    - **New** **tab** → Press <Ctrl> + Click (Windows) or <Cmd> + Click (Mac).

### Cache Storage

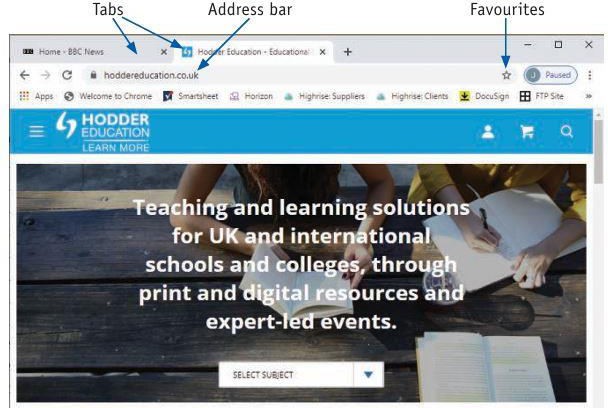
* + Browsers store **cached** **data** (temporary files like images and scripts) to load websites faster on repeat visits.
  + This reduces the need to download the same content multiple times.

### JavaScript Support

* + Web browsers can execute **JavaScript**, a programming language used to create **interactive** and **dynamic** web pages.
  + Example: Forms, animations, and pop-up messages on websites are powered by JavaScript.

### Address Bar

* + The address bar is where users enter a website's **URL** **(Uniform** **Resource** **Locator)**.
  + Some browsers provide **search** **suggestions** directly from the address bar.



## A-Rated Questions/Answers By Examiner

### Q1: What is a web browser, and what is its main function?

**Answer:** A web browser is a **software** **application** used to access, retrieve, and display web pages on the **World** **Wide** **Web** **(WWW)**. Its main function is to interpret and render HTML documents, allowing users to **view** **websites,** **navigate** **links,** **and** **interact** **with** **online** **content**.

### Q2: What are bookmarks in a web browser, and why are they useful?

**Answer:** Bookmarks (also called **favorites**) are stored shortcuts to frequently visited websites. They are useful because they allow users to **quickly** **access** **saved** **web** **pages** without needing to retype the URL.

### Q3: Explain how web browsers use cookies.

**Answer:** Cookies are **small** **text** **files** stored on a user's device by websites. They are used to:

1. **Remember** **login** **details** (e.g., staying signed in).
2. **Store** **user** **preferences** (e.g., language settings).
3. **Track** **user** **activity** for personalized recommendations (e.g., targeted ads).

### Q4: What is the purpose of cache storage in a web browser?

**Answer:** Cache storage temporarily saves **website** **data** (such as images, scripts, and stylesheets) on the user's device. This helps:

* + **Load** **web** **pages** **faster** on repeat visits.
  + **Reduce** **bandwidth** **usage** by avoiding repeated downloads.

### Improve browsing performance.

**Q5:** **How** **can** **a** **user** **open** **a** **hyperlink** **in** **a** **new** **tab?** **Answer:** A user can open a hyperlink in a new tab by:

* + Holding <Ctrl> (Windows) or <Cmd> (Mac) and clicking the link.
  + Right-clicking the link and selecting **"Open** **in** **new** **tab."**

## Write your Answers on your Notebook and Verify it on Next Screen

**Q6:** **What** **are** **private** **browsing** **modes,** **and** **how** **do** **they** **work?**

**Q7:** **What** **is** **a** **browser** **extension,** **and** **how** **does** **it** **enhance** **web** **browsing?**

**Q8:** **What** **is** **a** **web** **browser’s** **user** **agent,** **and** **what** **is** **its** **purpose?**

**Q9:** **What** **are** **some** **common** **web** **browsers,** **and** **how** **do** **they** **differ?**

**Q10:** **How** **do** **web** **browsers** **handle** **security** **threats?**

* 1. **Answer:**

1. Private browsing (e.g., Incognito Mode in Chrome, Private Window in Firefox) prevents the browser from saving browsing history, cookies, and site data.
2. It helps users browse without leaving traces on their device.
3. However, private mode does not make users anonymous—ISPs and websites can still track activity.
4. It is useful for logging into multiple accounts or browsing sensitive information.

### Answer:

1. A browser extension is a small software add-on that enhances browser functionality.
2. It allows users to customize their browsing experience (e.g., ad blockers, password managers, productivity tools).
3. Extensions run in the background and integrate with the browser to provide extra features.
4. They are available on browser-specific stores, such as the Chrome Web Store or Firefox Add-ons.

### Answer:

1. A user agent is a string of text sent by the browser to websites, identifying the browser type and operating system.
2. Websites use user agents to adjust content for different devices and browsers.
3. Example: A mobile website version may be displayed when a user agent indicates a smartphone.
4. Developers can modify user agents for testing website compatibility.

### Answer:

1. **Google** **Chrome** – Fast, widely used, supports many extensions.
2. **Mozilla** **Firefox** – Privacy-focused, open-source, customizable.
3. **Microsoft** **Edge** – Built on Chromium, integrated with Windows.
4. **Apple** **Safari** – Optimized for macOS and iOS, energy-efficient.
5. **Opera** – Built-in VPN and ad blocker, customizable UI.

### Answer:

1. **Phishing** **protection** – Warns users about suspicious websites.
2. **Sandboxing** – Isolates web pages to prevent malicious code from affecting the system.
3. **Automatic** **updates** – Patches security vulnerabilities.
4. **Blocking** **insecure** **content** – Prevents mixed-content loading (HTTP content on HTTPS sites).
5. **Permission** **controls** – Asks users before allowing access to the camera, microphone, or location.

# Topic: Retrieval and location of web pages

Reading Time: 15 mins

## Note\* Highlight important/core points while reading

* + Read the content and write the answers given in the document in your words, to get the solid grip on topic.

### Retrieval and Location of Web Pages

When a user wants to access a website, their computer must **locate** **the** **correct** **web** **server** that stores the requested web pages. This process involves the **Domain** **Name** **System** **(DNS)**, which translates human-readable web addresses (**URLs**) into machine- readable **IP** **addresses**.

### Step-by-Step Process of Web Page Retrieval

1. **User** **Requests** **a** **Web** **Page**
   * The user **opens** **a** **web** **browser** and enters a website URL (e.g., [www.hoddereducation.co.uk).](http://www.hoddereducation.co.uk/)
   * The browser does not understand domain names directly, so it needs the corresponding **IP** **address** of the website.

### Querying the Domain Name System (DNS)

* + The browser asks a **DNS** **server** **(1)** for the IP address of [www.hoddereducation.co.uk.](http://www.hoddereducation.co.uk/)
  + The DNS server (1) checks its **database/cache** to see if it has the IP address stored.

### Resolving the IP Address

* + If **DNS** **server** **(1)** **does** **not** **have** **the** **IP** **address**, it **forwards** **the** **request** to another **DNS** **server** **(2)**.
  + The **DNS** **server** **(2)** finds the matching **IP** **address** **(107.162.140.19)** and sends it back to **DNS** **server** **(1)**.
  + **DNS** **server** **(1)** **now** **stores** this information in its cache for faster future access.

### Returning the IP Address to the Browser

* + **DNS** **server** **(1)** **sends** **the** **resolved** **IP** **address** (107.162.140.19) back to the user's computer.
  + The browser can now communicate directly with the website’s **web** **server**.

### Establishing a Connection and Retrieving Web Pages

* + The browser **sends** **a** **request** to the web server at **107.162.140.19**.
  + The web server processes the request and sends back the required **HTML** **files,** **images,** **CSS,** **and** **JavaScript**.
  + The browser **interprets** **the** **HTML** **and** **other** **web** **page** **elements** to display the content to the user.

### Role of the Domain Name System (DNS)

The **DNS** is an essential part of the Internet. It acts like a **phonebook**, mapping **domain** **names** **to** **IP** **addresses**.

* + Without DNS, users would need to remember numeric IP addresses instead of simple domain names.
  + DNS servers communicate with each other to resolve website addresses efficiently.

## A-Rated Questions/Answers By Examiner

### Q1: What is the purpose of a DNS server in web browsing?

**Answer:** A **Domain** **Name** **System** **(DNS)** **server** translates **human-readable** **domain** **names** (e.g., [www.google.com)](http://www.google.com/) into **numeric** **IP** **addresses** (e.g., 142.250.180.46).

This allows browsers to locate and retrieve web pages from the correct server.

### Q2: Describe the step-by-step process of retrieving a web page. Answer:

1. **User** **enters** **a** **URL** in the web browser.
2. The browser asks a **DNS** **server** for the IP address of the website.
3. If the first DNS server doesn’t have the IP, it queries another **DNS** **server**.
4. Once the IP address is found, it is sent back to the user’s computer.
5. The browser **establishes** **a** **connection** with the web server and requests the web page.
6. The web server sends **HTML** **files** and other content to the browser.
7. The browser **interprets** **and** **displays** the web page to the user.

### Q3: Why do DNS servers store information in a cache?

**Answer:** DNS servers use a **cache** to store previously resolved domain names and IP addresses. This:

* + **Speeds** **up** **future** **access** to frequently visited websites.
  + **Reduces** **network** **traffic** by avoiding repeated DNS lookups.
  + **Improves** **overall** **performance** of web browsing.

**Q4:** **What** **happens** **if** **a** **DNS** **server** **cannot** **find** **an** **IP** **address** **in** **its** **database?** **Answer:** If a **DNS** **server** cannot find an IP address in its database, it:

1. **Forwards** **the** **request** to another DNS server.
2. If the second DNS server finds the IP address, it returns it to the first DNS server.
3. The first DNS server **stores** **the** **IP** **address** in its cache for future use.
4. The IP address is sent to the user's computer, which then contacts the web server.

### Q5: What is the role of HTML in displaying web pages?

**Answer:** **HTML** **(Hypertext** **Markup** **Language)** is the standard language used to structure web pages. It:

* + Defines the **content** **and** **layout** of a web page.
  + Works alongside **CSS** (for styling) and **JavaScript** (for interactivity).
  + Is interpreted by the web browser to display text, images, links, and multimedia elements.

## Write your Answers on your Notebook and Verify it on Next Screen

**Q6:** **What** **is** **an** **IP** **address,** **and** **why** **is** **it** **important** **in** **web** **browsing?**

**Q7:** **What** **is** **the** **difference** **between** **IPv4** **and** **IPv6?**

**Q8:** **What** **happens** **if** **a** **DNS** **server** **is** **down** **or** **unreachable?**

**Q9:** **What** **is** **a** **recursive** **DNS** **query,** **and** **how** **does** **it** **work?**

**Q10:** **How** **do** **CDN** **(Content** **Delivery** **Networks)** **affect** **web** **page** **retrieval?**

1. **Answer:**
2. An IP (Internet Protocol) address is a unique numerical label assigned to each device connected to the internet.
3. It allows devices to identify and communicate with each other over the network.
4. Websites have IP addresses that browsers use to locate and retrieve web pages.
5. Example: Instead of typing "[www.google.com](http://www.google.com/)," users could enter "142.250.180.46" (Google's IP), but DNS makes it easier by translating domain names to IP addresses.

### Answer:

1. **IPv4** **(Internet** **Protocol** **version** **4):**
   * Uses a 32-bit address system (e.g., 192.168.1.1).
   * Can support about 4.3 billion unique addresses.
   * Due to high internet growth, IPv4 addresses are running out.

### IPv6 (Internet Protocol version 6):

* + Uses a 128-bit address system (e.g., 2001:0db8:85a3::8a2e:0370:7334).
  + Provides an almost limitless number of addresses.
  + Improves efficiency, security, and device communication.

### Answer:

1. If a DNS server is down, the browser cannot resolve domain names to IP addresses.
2. Users may see an error message like "DNS Server Not Responding."
3. The computer may try an alternative DNS server (if configured).
4. Solutions include switching to a different DNS provider (e.g., Google DNS: 8.8.8.8, Cloudflare DNS: 1.1.1.1) or checking the internet connection.

### Answer:

1. A **recursive** **DNS** **query** is when a DNS server takes full responsibility for finding an IP address.
2. If the first DNS server does not have the answer, it contacts other servers on behalf of the user.
3. The query goes through:
   * **Recursive** **Resolver** → Contacts other DNS servers.
   * **Root** **DNS** **Server** → Directs to a Top-Level Domain (TLD) server.
   * **TLD** **Server** → Directs to the authoritative DNS server.
   * **Authoritative** **DNS** **Server** → Provides the final IP address.
4. The resolved IP address is returned to the user's browser.

### Answer:

1. **CDNs** store copies of web content on multiple servers worldwide.
2. When a user requests a page, the content is delivered from the nearest CDN server instead of the original web server.

### Benefits:

* + Faster loading speeds.
  + Reduced server load.
  + Improved reliability and availability.
  + Better performance for users in different geographical locations.

1. Examples: Cloudflare, Akamai, Amazon CloudFront.

# Topic: Cookies

Reading Time: 15 mins

## Note\* Highlight important/core points while reading

* Read the content and write the answers given in the document in your words, to get the solid grip on topic.

### Cookies

Cookies are **small** **text** **files** stored on a user’s computer or device by websites they visit. They help websites remember users' preferences, login details, and browsing history, improving the user experience.

### Types of Cookies

1. **Session** **Cookies**
   * Temporary cookies that **expire** **when** **the** **user** **closes** **the** **browser**.
   * Used for **temporary** **storage**, such as remembering login sessions or shopping cart items.
   * Example: When a user logs into a website, a session cookie keeps them logged in until they close the browser.

### Persistent (Permanent) Cookies

* + Stored on the user’s device **even** **after** **the** **browser** **is** **closed**.
  + Used to **remember** **user** **preferences** **and** **login** **details** for future visits.
  + Can be deleted manually or expire after a set time.
  + Example: A website remembers a user’s preferred language or login credentials.

### How Cookies Work in Web Browsing First Time the User Logs into a Website

1. The user enters their **username** **and** **password** on a website.
2. The website **stores** **a** **cookie** on the user’s computer with login credentials or preferences.
3. The session cookie remains active until the user logs out or closes the browser.
4. If persistent cookies are used, the website can remember login details for future visits.

### User Logs into the Website Again

1. The browser checks for **stored** **cookies** from the website.
2. If a **persistent** **cookie** exists, the website automatically logs the user in or applies their saved settings.
3. The user does not have to **re-enter** **their** **credentials** unless the cookie has expired or been deleted.

**Uses** **of** **Persistent** **Cookies**

**Function** **Explanation**

**Remember** **login** **details**

**Personalized** **experience**

**Shopping** **cart** **memory**

**Tracking** **internet** **habits**

Saves usernames, passwords, and email addresses for easier future logins.

Recognizes users and applies saved preferences (e.g., dark mode, preferred language).

Saves items in an online shopping cart, even after the browser is closed.

Monitors user browsing history to improve recommendations.

**Targeted** **advertising** Displays ads based on previous searches or purchases.

**Online** **transactions** Used in e-commerce and online banking for security and session

management.

### Online gaming progress

**Social** **media** **preferences**

Stores game progress and settings.

Saves preferences like news feed settings or frequently visited profiles.

## A-Rated Questions/Answers By Examiner

### Q1: What are cookies, and why are they used in web browsing? Answer:

Cookies are **small** **text** **files** stored on a user's device by websites. They are used to:

### Remember login details and preferences.

1. **Store** **shopping** **cart** **items**.
2. **Track** **user** **activity** for personalized recommendations.
3. **Improve** **website** **functionality** and security.

### Q2: What is the difference between session cookies and persistent cookies? Answer:

* + **Session** **cookies** → Temporary, expire when the browser is closed, used for login

sessions.

* + **Persistent** **cookies** → Stored permanently, used for remembering user preferences

and login details.

**Q3:** **How** **do** **persistent** **cookies** **improve** **the** **user** **experience?** **Answer:** Persistent cookies:

1. **Automatically** **log** **users** **in** without re-entering credentials.
2. **Remember** **shopping** **cart** **items** for later purchases.
3. **Store** **website** **preferences** like language or theme settings.
4. **Enable** **personalized** **ads** based on browsing history.

**Q4:** **How** **are** **cookies** **used** **in** **online** **shopping?** **Answer:** Cookies help online shopping by:

1. **Saving** **items** **in** **the** **shopping** **cart** even after the user leaves the website.
2. **Remembering** **billing** **and** **shipping** **details** for faster checkout.
3. **Providing** **product** **recommendations** based on previous purchases.

### Q5: Why do some websites ask users to accept cookies?

**Answer:** Websites ask users to accept cookies due to **privacy** **laws** **(e.g.,** **GDPR)**. This ensures users are informed about:

* + What data is collected.
  + How their browsing activity is tracked.
  + Options to accept, reject, or manage cookie settings.

## Write your Answers on your Notebook and Verify it on Next Screen

**Q6:** **What** **are** **third-party** **cookies,** **and** **how** **do** **they** **differ** **from** **first-party** **cookies?**

**Q7:** **How** **can** **users** **manage** **or** **delete** **cookies** **in** **their** **web** **browsers?**

**Q8:** **What** **are** **supercookies,** **and** **why** **are** **they** **considered** **a** **security** **risk?**

**Q9:** **How** **do** **websites** **use** **cookies** **for** **security** **purposes?**

**Q10:** **What** **is** **the** **impact** **of** **GDPR** **and** **other** **privacy** **laws** **on** **cookie** **usage?**

1. **Answer:**
   1. **First-party** **cookies** → Created by the website the user is visiting; used for login

details, preferences, and user experience.

* 1. **Third-party** **cookies** → Created by external websites (e.g., advertisers, analytics services) embedded on the visited site; used for tracking user behavior across multiple websites.
  2. Example:
     + A cookie from *amazon.com* remembering a user’s shopping cart (first-party).
     + A tracking cookie from *adnetwork.com* following a user’s activity across different sites (third-party).

### Answer:

* 1. Users can manage cookies through their browser settings.
  2. Options typically include:
     + **Blocking** **all** **cookies** → Prevents websites from storing data.
     + **Clearing** **cookies** → Deletes stored cookies manually.
     + **Enabling** **‘Do** **Not** **Track’** → Requests websites not to track user activity.
     + **Managing** **site-specific** **cookies** → Allowing or blocking cookies for specific

websites.

* 1. Example: In Google Chrome → Settings > Privacy and Security > Cookies and other

site data.

### Answer:

* 1. **Supercookies** are more persistent tracking mechanisms stored at a deeper system level, such as in Flash storage or HTTP headers.
  2. Unlike regular cookies, they are harder to delete and can track users across different browsing sessions.

### Risks:

* + - Harder to remove, even after clearing browser cookies.
    - Used for extensive tracking without user consent.
    - Can be exploited for cyberattacks or unauthorized data collection.

### Answer:

* 1. **Session** **management** → Ensures users remain logged in securely.
  2. **Authentication** → Prevents unauthorized access by verifying user credentials.
  3. **Fraud** **prevention** → Detects unusual login attempts or payment fraud.
  4. **CSRF** **(Cross-Site** **Request** **Forgery)** **protection** → Secure cookies help prevent

attacks where malicious sites trick users into making unauthorized requests.

### Answer:

* 1. **General** **Data** **Protection** **Regulation** **(GDPR)** and **California** **Consumer** **Privacy** **Act** **(CCPA)** require websites to:
     + Inform users about cookie usage.
     + Obtain user consent before storing cookies.
     + Provide options to opt-out or manage cookie preferences.
  2. Websites often display cookie consent pop-ups to comply with these laws.
  3. Some browsers (e.g., Safari, Firefox) have introduced restrictions on third-party cookies for enhanced privacy.

# Topic: Digital Currency

Reading Time: 15 mins

## Note\* Highlight important/core points while reading

* Read the content and write the answers given in the document in your words, to get the solid grip on topic.

### What is Digital Currency?

Digital currency is a **form** **of** **money** **that** **exists** **only** **in** **electronic** **form**. Unlike physical cash (banknotes and coins), digital currencies are stored in **digital** **wallets** and used for transactions through the **internet**.

There are **two** **main** **types** of digital currency:

1. **Traditional** **Digital** **Currency** (regulated by governments and banks)
2. **Cryptocurrency** (decentralized and based on blockchain technology)

### Fiat Currency and Central Banking System

1. **Fiat** **Currency**
   * **Fiat** **currency** is **government-issued** money (e.g., USD, GBP, EUR).
   * It is **not** **backed** **by** **a** **physical** **commodity** like gold or silver.
   * The **value** **of** **fiat** **currency** is determined by the **government** **and** **central** **banks** based on economic conditions.

### Central Banking System

* + The **central** **bank** (e.g., Federal Reserve, European Central Bank) controls fiat currency.
  + It **regulates** **inflation,** **interest** **rates,** **and** **money** **supply** to stabilize the economy.
  + **Traditional** **digital** **currencies** (like online banking transactions) are controlled by the **central** **banking** **system**.

### Cryptocurrency and Its Differences from Traditional Digital Currency

**Feature** **Traditional** **Digital** **Currency** **Cryptocurrency**

**Control** Central banks & governments regulate transactions.

**Transparency** Transactions are private between banks

and users.

**Security** Banks use centralized databases

(vulnerable to hacking).

**Transaction** **Speed** Can take hours or days (especially for

international transactions).

Decentralized; controlled by a peer-to- peer network.

Transactions are **publicly** **recorded** on a blockchain.

Uses **blockchain** **technology** for high security.

Faster transactions (sometimes in minutes).

### Tracking & Monitoring

Banks track and control all transactions.

Transactions are **anonymous** **but** **publicly** **visible** on a blockchain.

### How Cryptocurrency Works

1. **Use** **of** **Cryptography**
   * Cryptocurrency uses **cryptographic** **techniques** to **secure** **transactions**.
   * Each transaction is verified using **complex** **mathematical** **algorithms**.

### Decentralization

* + Unlike traditional currency, cryptocurrency **is** **not** **controlled** **by** **any** **central** **authority**.
  + The **community** (miners, developers, and users) decides the rules.

### Blockchain Technology

* + Cryptocurrency operates on a **blockchain**, which is a **decentralized** **ledger**.
  + Every transaction is **recorded** **on** **multiple** **computers** (nodes), making it **highly** **secure** **and** **tamper-proof**.

### Transparency & Security

* + Every cryptocurrency transaction is **publicly** **recorded**, preventing fraud.
  + Blockchain ensures that transactions **cannot** **be** **altered** once verified.

## A-Rated Questions/Answers By Examiner

### Q1: What is digital currency?

**Answer:** Digital currency is a form of money that exists **only** **in** **electronic** **form**. It includes:

* + **Traditional** **digital** **currency** (controlled by banks and governments).
  + **Cryptocurrency** (decentralized and based on blockchain).

### Q2: How is cryptocurrency different from traditional digital currency?

**Answer:** **Cryptocurrency** **is** **decentralized**, while traditional digital currency is **controlled** **by** **central** **banks**.

* + **Cryptocurrency** **transactions** **are** **public** (on a blockchain), but **bank** **transactions** **are** **private**.
  + **Cryptocurrency** **has** **no** **government** **control**, while traditional digital currency is **regulated** **by** **financial** **institutions**.

**Q3:** **What** **is** **the** **role** **of** **cryptography** **in** **cryptocurrency?** **Answer:** Cryptography is used to:

1. **Secure** **transactions** and prevent fraud.
2. **Verify** **ownership** of cryptocurrency.
3. **Ensure** **data** **privacy** through encryption.

### Q4: What is blockchain, and how does it secure cryptocurrency?

**Answer:** Blockchain is a **decentralized,** **digital** **ledger** that records all cryptocurrency transactions. It ensures security by:

1. Storing data **across** **multiple** **computers** (making it tamper-proof).
2. **Verifying** **each** **transaction** through cryptographic algorithms.
3. Preventing **fraud** **and** **double-spending**.

**Q5:** **Why** **do** **some** **people** **prefer** **cryptocurrency** **over** **fiat** **currency?** **Answer:** People prefer cryptocurrency because:

1. **It** **is** **decentralized** (not controlled by governments).
2. **Transactions** **are** **fast** and global.
3. **It** **is** **more** **secure** due to blockchain technology.
4. **It** **provides** **financial** **privacy** and prevents third-party interference.

## Write your Answers on your Notebook and Verify it on Next Screen

**Q6:** **What** **are** **the** **advantages** **of** **digital** **currency** **over** **physical** **cash?**

**Q7:** **What** **are** **some** **common** **uses** **of** **cryptocurrency?**

**Q8:** **What** **are** **the** **risks** **associated** **with** **cryptocurrency?**

**Q9:** **What** **is** **the** **difference** **between** **Bitcoin** **and** **Ethereum?**

**Q10:** **What** **are** **stablecoins,** **and** **how** **do** **they** **work?**

1. **Answer:**
   1. **Convenience** → Digital currency allows instant online transactions without handling

physical money.

* 1. **Security** → Reduces the risk of theft or loss compared to carrying cash.
  2. **Global** **Transactions** → Enables cross-border payments with minimal fees and faster processing times.
  3. **Efficiency** → Streamlines financial transactions, reducing reliance on physical

banking infrastructure.

* 1. **Tracking** **&** **Transparency** → Digital transactions create records that can help

prevent fraud and enhance accountability.

### Answer:

* 1. **Online** **purchases** → Many businesses accept cryptocurrencies as payment (e.g.,

Tesla, Microsoft).

* 1. **Investment** → People buy cryptocurrencies as an asset, hoping for long-term value appreciation.
  2. **Remittances** → Sending money across borders without high fees or long

processing times.

* 1. **Decentralized** **finance** **(DeFi)** → Allows users to earn interest, lend, and borrow

without banks.

* 1. **Smart** **contracts** → Automates agreements without intermediaries (e.g., Ethereum

blockchain).

### Answer:

1. **Volatility** → Prices can fluctuate rapidly, leading to financial losses.
2. **Lack** **of** **regulation** → No central authority to protect users from fraud or scams.
3. **Security** **risks** → If a wallet's private key is lost or stolen, funds cannot be

recovered.

1. **Illegal** **activities** → Some criminals use cryptocurrency for money laundering or

illicit transactions.

1. **Scalability** **issues** → Some blockchains struggle with high transaction volumes,

leading to delays and high fees.

|  |  |  |
| --- | --- | --- |
| **9.** **Answer:** |  | |
| **Answer:**  **Feature** | **Bitcoin** | **Ethereum** |
| **Purpose** | Digital currency | Smart contracts & decentralized apps (dApps) |
| **Blockchain** | Bitcoin blockchain | Ethereum blockchain |

**Transaction** **speed** Slower (10 minutes per

block)

Faster (seconds to minutes)

### Smart contract support

No Yes

**Supply** **limit** 21 million coins No fixed limit

### Answer:

* 1. **Stablecoins** are cryptocurrencies designed to maintain a stable value by being pegged to an asset like the US dollar or gold.

### Types of stablecoins:

* + - **Fiat-backed** → Supported by real-world currency (e.g., USDT, USDC).
    - **Crypto-backed** → Backed by other cryptocurrencies as collateral (e.g., DAI).
    - **Algorithmic** → Uses smart contracts to control supply and maintain price

stability.

* 1. **Use** **cases:** Stablecoins are used for payments, trading, and remittances without volatility.

# Topic: Blockchaining

Reading Time: 15 mins

## Note\* Highlight important/core points while reading

* Read the content and write the answers given in the document in your words, to get the solid grip on topic.

### What is Blockchain?

Blockchain is a **decentralized,** **digital** **ledger** that records transactions across multiple computers in a secure, transparent, and tamper-proof way. Each transaction is stored in a **block** and linked to the previous block, forming a **chain** **of** **blocks**—hence the

name **blockchain**.

### Key Features of Blockchain

**Decentralization** – No central authority controls the data. **Transparency** – Everyone in the network can verify transactions. **Security** – Transactions cannot be altered once recorded.

**Immutability** – Data is permanent and cannot be deleted.

### How Blockchain Works

1. **A** **transaction** **is** **initiated.** (e.g., sending cryptocurrency).
2. **The** **transaction** **is** **verified** by nodes (computers) in the blockchain network.

### The verified transaction is added to a new block.

1. **Proof-of-work** (or another consensus mechanism) validates the block.
2. **The** **block** **is** **linked** **to** **the** **previous** **block**, forming a chain.

### The transaction is now permanently recorded. Key Concepts in Blockchain

1. **Cryptocurrency** **&** **Digital** **Currency** **Exchanges**
   * Blockchain is the foundation of cryptocurrencies like **Bitcoin** **and** **Ethereum**.
   * **Cryptocurrency** **exchanges** allow users to trade digital currencies securely.
   * Transactions are stored on the blockchain, making them **transparent** **and** **secure**.

### Smart Contracts

* + **Smart** **contracts** are **self-executing** **contracts** with terms written in code.
  + They automatically execute when conditions are met, removing the need for intermediaries.
  + Example: In real estate, a smart contract could release payment when ownership is transferred.

### Blockchain in Research (Pharmaceutical Industry)

* + Helps track **drug** **supply** **chains** to prevent counterfeit medicine.
  + Stores **clinical** **trial** **data** securely to ensure transparency.
  + Provides **timestamped** **records** for scientific research.

### Blockchain in Politics

* + Used for **secure** **digital** **voting**, preventing election fraud.
  + Increases transparency by making **government** **spending** **records** public.
  + Ensures political documents **cannot** **be** **altered** **or** **deleted**.

### Blockchain in Education

* + **Degree** **verification** – Universities can store diplomas on the blockchain.
  + **Timestamping** **research** **papers** – Ensures original authorship and prevents plagiarism.
  + **Secure** **student** **records** – Permanent and accessible worldwide.

### Important Blockchain Terms

1. **Timestamp**
   * Every transaction in a blockchain has a **timestamp**, ensuring it is recorded at an exact time.
   * This prevents fraud and **proves** **ownership** of digital assets.

### Genesis Block

* + The **first** **block** in a blockchain.
  + It contains the first transaction and serves as the foundation of the network.
  + Example: Bitcoin’s genesis block was created in **2009** **by** **Satoshi** **Nakamoto**.

### Proof-of-Work (PoW)

* + A **consensus** **mechanism** used to validate transactions.
  + Miners solve **complex** **mathematical** **problems** to add a new block.
  + Example: Bitcoin uses **PoW** **mining**, where miners compete to solve problems and earn rewards.

## A-Rated Questions/Answers By Examiner

### Q1: What is blockchain, and how does it work?

**Answer:** Blockchain is a **decentralized** **digital** **ledger** that records transactions securely. It works by:

1. Storing data in **blocks** linked together.
2. Using **nodes** to verify transactions.
3. Applying **consensus** **mechanisms** (like proof-of-work) for validation.
4. Keeping data **permanent** **and** **tamper-proof**.

### Q2: What is a smart contract, and how does it work?

**Answer:** A smart contract is a **self-executing** **program** stored on the blockchain. It automatically runs when conditions are met.

Example: A smart contract in **real** **estate** can release payment when property ownership is transferred.

**Q3:** **What** **is** **the** **purpose** **of** **the** **genesis** **block** **in** **blockchain?** **Answer:** The **genesis** **block** is the **first** **block** in a blockchain. It:

### Initiates the blockchain.

* + **Contains** **the** **first** **transaction**.
  + **Serves** **as** **the** **foundation** for all future transactions.

**Q4:** **How** **is** **blockchain** **used** **in** **politics?** **Answer:** Blockchain improves politics by:

1. **Enabling** **secure** **digital** **voting** (prevents election fraud).
2. **Tracking** **government** **spending** (transparency).
3. **Protecting** **official** **documents** (tamper-proof storage).

### Q5: What is proof-of-work, and why is it important in blockchain?

**Answer:** Proof-of-work (PoW) is a **consensus** **mechanism** where miners solve **complex** **mathematical** **problems** to verify transactions. It:

* + **Prevents** **fraud** by making it costly to alter the blockchain.
  + **Ensures** **decentralization** by removing central authority control.

**Rewards** **miners** with cryptocurrency for their efforts.

## Write your Answers on your Notebook and Verify it on Next Screen

**Q6:** **How** **does** **decentralization** **in** **blockchain** **improve** **security** **and** **transparency?**

**Q7:** **What** **are** **the** **main** **differences** **between** **public** **and** **private** **blockchains?**

**Q8:** **How** **is** **blockchain** **transforming** **the** **supply** **chain** **industry?**

**Q9:** **What** **is** **the** **role** **of** **cryptocurrency** **mining** **in** **blockchain** **networks?**

**Q10:** **How** **does** **blockchain** **technology** **impact** **cybersecurity?**

1. **Answer:** Decentralization ensures that no single entity controls the network, making it resistant to hacking and fraud. Transparency is achieved because all participants can view and verify transactions on the public ledger.

### Answer:

* + **Public** **Blockchain**: Open to anyone, decentralized, and secured by consensus mechanisms like proof-of-work. Example: Bitcoin, Ethereum.
  + **Private** **Blockchain**: Restricted access, controlled by an organization, used for internal transactions. Example: Hyperledger Fabric.

1. **Answer:** Blockchain enhances supply chains by:
2. Providing real-time tracking of goods.
3. Ensuring authenticity by verifying product origins.
4. Reducing fraud and counterfeiting through tamper-proof records.
5. **Answer:** Mining involves validating transactions and adding them to the blockchain. Miners solve cryptographic puzzles (proof-of-work) to secure the network and earn rewards in the form of cryptocurrency.
6. **Answer:** Blockchain enhances cybersecurity by:
7. Preventing data tampering with immutable records.
8. Using encryption to secure transactions.
9. Reducing the risk of identity theft through decentralized identity management.

# Topic: Cyber security threats

Reading Time: 15 mins

## Note\* Highlight important/core points while reading

* + Read the content and write the answers given in the document in your words, to get the solid grip on topic.

### Cyber Security Threats

Cyber security threats refer to **any** **malicious** **activity** that attempts to damage, steal, or gain unauthorized access to computer systems, networks, or data. These threats can come from hackers, malware, and various cyberattacks.

### Types of Cyber Security Threats

1. **Brute** **Force** **Attacks**
   * A **trial-and-error** **method** used to guess passwords.
   * The attacker systematically tries different combinations until the correct one is found.
   * Automated software can try **millions** **of** **passwords** **per** **second**.
   * **Prevention:** Use strong passwords with uppercase, lowercase, numbers, and special characters.

### Data Interception (Man-in-the-Middle Attack)

* + Data is **intercepted** while being transferred over a network.
  + Attackers **steal** **sensitive** **information** (e.g., login credentials, financial data).
  + Often happens on **public** **Wi-Fi** **networks**.
  + **Prevention:** Use **encrypted** **connections** **(HTTPS,** **VPNs)** and avoid public Wi-Fi for sensitive transactions.

### Distributed Denial of Service (DDoS) Attacks

* + Attackers use **multiple** **computers** **(botnets)** to send overwhelming traffic to a website or network.
  + The target system **becomes** **slow** **or** **crashes**, making it unavailable for users.
  + Often used to **disrupt** **businesses,** **banks,** **and** **government** **services**.

### Prevention: Use firewalls, load balancers, and traffic filtering tools.

1. **Hacking**
   * The act of **gaining** **unauthorized** **access** to computer systems or networks.
   * **Black-hat** **hackers** exploit security vulnerabilities for **malicious** **purposes**.
   * **White-hat** **hackers** help identify weaknesses to **improve** **security**.
   * **Prevention:** Regular **software** **updates**, **strong** **authentication**, and **intrusion** **detection** **systems** **(IDS)**.

### Malware (Malicious Software)

Malware is **software** **designed** **to** **harm** or exploit a computer system. Types include:

### Type Description

**Viruses** Attach to legitimate files and spread when opened.

**Worms** Self-replicating malware that spreads without user action.

**Trojan** **Horse** Disguised as legitimate software but has a hidden malicious function.

**Spyware** Secretly collects user data (e.g., keystrokes, login details).

**Adware** Displays unwanted advertisements, often leading to malicious sites.

**Ransomware** Encrypts user files and demands a ransom for decryption.

* **Prevention:** Use **antivirus** **software**, avoid suspicious downloads, and enable **firewall** **protection**.

### Phishing

* + A cyberattack where hackers **trick** **users** **into** **giving** **personal** **information** (e.g., passwords, credit card details).
  + Usually done via **fake** **emails** **or** **websites** pretending to be legitimate.
  + Example: An email from “your bank” asking you to reset your password on a **fake** **website**.

### Prevention:

* + - Verify sender emails before clicking links.
    - Never enter credentials on unknown websites.
    - Use **email** **spam** **filters**.

### Pharming

* + Redirects users from a legitimate website to a **fake,** **malicious** **website**.
  + Users **unknowingly** **enter** login credentials on the fake site.
  + Often used to **steal** **banking** **details**.

### Prevention:

* + - Use **DNS** **protection** **software**.
    - Always check the URL before entering sensitive data.
    - Enable **multi-factor** **authentication** **(MFA)**.

### Social Engineering

* + Attackers manipulate people into **revealing** **confidential** **information**.
  + Methods include:
    - **Pretexting**: Pretending to be a trusted person to get information.
    - **Baiting**: Offering something attractive (e.g., a free download) to trick users into installing malware.
    - **Tailgating**: Following someone into a restricted area without proper authentication.

### Prevention:

* + - Always verify identities before sharing information.
    - Educate employees about security awareness.
    - Implement **access** **controls** for sensitive data.

## A-Rated Questions/Answers By Examiner

### Q1: What is a brute force attack, and how can it be prevented?

**Answer:** A **brute** **force** **attack** is a method where an attacker repeatedly tries different password combinations until they guess the correct one.

### Prevention:

* + Use **strong** **passwords** with uppercase, lowercase, numbers, and symbols.
  + Enable **account** **lockout** after multiple failed attempts.

### Use two-factor authentication (2FA).

**Q2:** **What** **is** **a** **DDoS** **attack,** **and** **how** **does** **it** **affect** **websites?**

**Answer:** A **DDoS** **(Distributed** **Denial** **of** **Service)** **attack** floods a website with excessive traffic, causing it to slow down or crash.

### Effects:

* + Websites become **unavailable** to users.
  + Businesses lose revenue and customers.
  + Servers may **overheat** **or** **fail**. **Prevention:**
  + Use **firewalls** **and** **traffic** **filters**.
  + Deploy **load** **balancing** to distribute traffic evenly.

### Q3: How does phishing work, and how can users protect themselves?

**Answer:** Phishing tricks users into revealing **sensitive** **information** through fake emails or websites.

### Protection:

* + Do not click on **unknown** **links** **or** **attachments**.
  + Verify website URLs before entering personal details.
  + Use **email** **spam** **filters**.

### Q4: What is ransomware, and why is it dangerous?

**Answer:** Ransomware is a **type** **of** **malware** that **encrypts** **user** **files** and demands payment to unlock them.

### Dangers:

* + Users **lose** **access** **to** **important** **files**.
  + Hackers may **delete** **or** **leak** **sensitive** **data**. **Prevention:**
  + Regularly **back** **up** **important** **files**.
  + Avoid clicking on **suspicious** **email** **links**.
  + Use **antivirus** **and** **firewall** **protection**.

### Q5: What is social engineering, and how do hackers use it? Answer:

Social engineering manipulates people into **revealing** **confidential** **information** by

pretending to be someone trustworthy.

### Examples:

* + **Pretexting**: Pretending to be an IT support person.
  + **Baiting**: Offering fake rewards (e.g., free software) to spread malware.

### Prevention:

* + Always verify identities before sharing information.
  + Train employees on cybersecurity awareness.
  + Use **access** **control** **measures** to protect data.

## Write your Answers on your Notebook and Verify it on Next Screen

**Q6:** **How** **does** **malware** **spread,** **and** **what** **are** **the** **best** **practices** **to** **prevent** **it?**

**Q7:** **What** **is** **the** **difference** **between** **phishing** **and** **pharming** **attacks?**

**Q8:** **How** **do** **hackers** **use** **man-in-the-middle** **(MITM)** **attacks,** **and** **how** **can** **they** **be** **prevented?**

**Q9:** **What** **are** **the** **risks** **of** **weak** **passwords,** **and** **how** **can** **users** **create** **strong** **ones?**

**Q10:** **How** **do** **organizations** **protect** **themselves** **from** **DDoS** **attacks?**

1. **Answer:** Malware spreads through infected email attachments, malicious websites, and software downloads.

### Prevention:

* + Avoid clicking on suspicious links or downloading unknown files.
  + Install and update antivirus software.
  + Enable firewalls to block unauthorized access.

### Answer:

* + **Phishing** tricks users into revealing personal data via fake emails or websites.
  + **Pharming** redirects users from legitimate websites to malicious ones without their knowledge.

**Prevention:** Verify URLs, use multi-factor authentication (MFA), and enable DNS security.

1. **Answer:** MITM attacks intercept communication between two parties to steal sensitive data.

### Prevention:

* + Use HTTPS and encrypted communication.
  + Avoid using public Wi-Fi for financial transactions.
  + Enable VPNs for secure data transmission.

1. **Answer:** Weak passwords can be easily cracked by brute force attacks, leading to data breaches.

### Best Practices for Strong Passwords:

* + Use a mix of uppercase, lowercase, numbers, and special characters.
  + Avoid common words or personal information.
  + Use a password manager for secure storage.

1. **Answer:** Organizations use various security measures to prevent DDoS attacks:
   * Deploy firewalls and intrusion detection systems (IDS).
   * Use content delivery networks (CDNs) to distribute traffic.
   * Implement rate limiting and load balancing to manage high traffic volumes.

# Topic: Keeping Data Safe from Security Threats

Reading Time: 20 mins

## Note\* Highlight important/core points while reading

* Read the content and write the answers given in the document in your words, to get the solid grip on topic.

### Keeping Data Safe from Security Threats

With the rise of cyber threats, it is crucial to implement security measures to protect sensitive data. Various methods such as **access** **levels,** **anti-malware,** **authentication,** **passwords,** **biometrics,** **firewalls,** **proxy** **servers,** **and** **privacy** **settings** help keep data safe.

1. **Access** **Levels**

Access levels control **who** **can** **view** **or** **modify** **data** in a system. There are usually four levels:

* 1. **Public** **Access**: Data accessible by **anyone** (e.g., company websites).
  2. **Friends**: Only people identified as ‘friends’ can see certain data (e.g., social media posts).
  3. **Custom**: Allows **further** **refinement** of data visibility (e.g., hiding posts from certain friends).
  4. **Data** **Owner**: Data only **visible** **to** **the** **owner** (e.g., personal financial records). *Access* *levels* *ensure* *that* *sensitive* *data* *is* *only* *visible* *to* *the* *right* *people,* *reducing* *unauthorized* *access* *risks.*

1. **Anti-Malware** **Software**

Anti-malware protects against **viruses,** **spyware,** **and** **other** **malicious** **software**. It operates using two methods:

* **Rules-based** **detection**: Looks for common spyware traits.
* **File** **structure** **analysis**: Identifies file patterns linked to spyware.

### Features of anti-spyware software:

* Detects and removes spyware.
* Blocks spyware downloads.
* Encrypts files to secure data.
* Encrypts keystrokes to prevent keylogging.
* Prevents unauthorized access to webcams and microphones.
* Warns users if personal data is stolen.

### Authentication

Authentication verifies user identity before granting access. Common methods include:

1. **Something** **you** **know** – Passwords or PINs.
2. **Something** **you** **have** – Security tokens, mobile phones.
3. **Something** **unique** **to** **you** – Biometrics (fingerprint, retina scans).

Using **multi-factor** **authentication** **(MFA)** enhances security by requiring multiple verification factors.

### Passwords and Usernames

Passwords secure access to **emails,** **online** **banking,** **shopping,** **and** **social** **media**.

### Best practices for password security:

* + Use **strong** **passwords** (at least one capital letter, number, and special character).
  + Change passwords **regularly**.
  + Avoid using easy-to-guess passwords (e.g., pet names).
  + Use **anti-spyware** **software** to prevent password theft. Example of a **strong** **password**: Sy12@#TT90kj=0 Example of a **weak** **password**: GREEN

### Biometrics

Biometric authentication uses **unique** **physical** **traits** to verify identity. Examples include:

* + **Fingerprint** **scans**
  + **Retina** **scans**
  + **Face** **recognition**
  + **Voice** **recognition**

Biometrics **improve** **security** by making authentication **difficult** **to** **fake**.

### Checking Email Spelling, Tone, and URL Links

* + Check for **spelling** **and** **grammatical** **errors** in emails.
  + **Legitimate** **companies** do not use generic email domains like @gmail.com.
  + Watch for **urgent** **or** **aggressive** **tone**—scammers try to create urgency.
  + Always **hover** **over** **links** to check the real URL before clicking. Example of a scam email:
  + Sent from: [support@paypal-secure.com](mailto:support@paypal-secure.com) (fake domain)
  + Subject: "URGENT: Your account will be suspended in 24 hours!"
  + Misspelled words and incorrect grammar

### Firewalls

A firewall is a **security** **system** that monitors and controls incoming/outgoing network traffic.

* + Examines traffic between the user’s device and the internet.
  + Blocks traffic that **does** **not** **meet** **security** **criteria**.
  + Can prevent access to **undesirable** **websites**.
  + Logs all network traffic for security audits.
  + Helps prevent **viruses** **and** **hacking** **attempts**.

Firewalls act as **barriers**, filtering harmful content and blocking cyber threats.

### Proxy Servers

A proxy server acts as an **intermediary** between a user and the internet.

* + Filters internet traffic, blocking harmful sites.
  + **Hides** **the** **user’s** **IP** **address** for anonymity.
  + Prevents direct access to web servers.

Protects against hacking and **Denial-of-Service** **(DoS)** **attacks**. **Caches** **web** **pages** to speed up browsing.

By **redirecting** **attacks** **away** from the user, proxy servers enhance security.

### Privacy Settings

Privacy settings help control **what** **data** **is** **shared** online.

* + **"Do** **Not** **Track"** **settings** prevent websites from collecting browsing data.
  + Check **saved** **payment** **methods** to reduce financial risks.
  + **Safe** **browsing** **alerts** warn about dangerous websites.
  + Manage **cookie** **settings** to control data tracking.

### Secure Sockets Layer (SSL)

SSL is an **encryption** **protocol** that secures online transactions.

* + Used for **banking,** **shopping,** **emails,** **and** **social** **media**.
  + Ensures that **data** **is** **encrypted** before transmission.
  + Prevents **man-in-the-middle** **attacks**.
  + Websites with SSL have a **padlock** **icon** and https:// in the URL.

Always ensure a website uses SSL before **entering** **sensitive** **information**.

### Type Description

**Viruses** Attach to legitimate files and spread when opened.

**Worms** Self-replicating malware that spreads without user action.

**Trojan** **Horse** Disguised as legitimate software but has a hidden malicious function.

**Spyware** Secretly collects user data (e.g., keystrokes, login details).

**Adware** Displays unwanted advertisements, often leading to malicious sites.

**Ransomware** Encrypts user files and demands a ransom for decryption.

* + **Prevention:** Use **antivirus** **software**, avoid suspicious downloads, and enable **firewall** **protection**.

### Phishing

* + A cyberattack where hackers **trick** **users** **into** **giving** **personal** **information** (e.g., passwords, credit card details).
  + Usually done via **fake** **emails** **or** **websites** pretending to be legitimate.
  + Example: An email from “your bank” asking you to reset your password on a **fake** **website**.

### Prevention:

* + Verify sender emails before clicking links.
  + Never enter credentials on unknown websites.
  + Use **email** **spam** **filters**.

### Pharming

* + Redirects users from a legitimate website to a **fake,** **malicious** **website**.
  + Users **unknowingly** **enter** login credentials on the fake site.
  + Often used to **steal** **banking** **details**.

### Prevention:

* + - Use **DNS** **protection** **software**.
    - Always check the URL before entering sensitive data.
    - Enable **multi-factor** **authentication** **(MFA)**.

### Social Engineering

* + Attackers manipulate people into **revealing** **confidential** **information**.
  + Methods include:
    - **Pretexting**: Pretending to be a trusted person to get information.
    - **Baiting**: Offering something attractive (e.g., a free download) to trick users into installing malware.
    - **Tailgating**: Following someone into a restricted area without proper authentication.

### Prevention:

* + - Always verify identities before sharing information.
    - Educate employees about security awareness.
    - Implement **access** **controls** for sensitive data.

## A-Rated Questions/Answers By Examiner

### Q1: What are the four access levels for data security? Answer:

1. **Public** **Access** – Data is accessible to anyone.
2. **Friends** – Only people marked as ‘friends’ can see the data.
3. **Custom** – Users can limit what friends see.
4. **Data** **Owner** – Only the owner has access.

**Q2:** **How** **does** **a** **firewall** **protect** **a** **computer** **system?** **Answer:** A firewall:

* + **Filters** **traffic** between a computer and the internet.
  + Blocks **suspicious** **data** that does not meet security criteria.
  + Prevents access to **unsafe** **websites**.
  + Logs network activity for security monitoring.
  + Helps **prevent** **hacking** **and** **malware** **infections**.

### Q3: What are two common methods used by anti-malware software to detect threats?

**Answer:**

1. **Rules-based** **detection** – Identifies malware by looking for common malicious traits.
2. **File** **structure** **analysis** – Recognizes malware based on suspicious file structures.

Anti-malware software detects, removes, and blocks spyware to **keep** **systems** **secure**. **Q4:** **How** **can** **a** **user** **identify** **a** **phishing** **email?**

### Answer:

* + **Look** **for** **spelling** **and** **grammar** **mistakes**.
  + **Check** **the** **sender’s** **email** **address**—legitimate companies use official domains.
  + **Be** **cautious** **of** **urgent** **language**—scammers create a false sense of urgency.
  + **Hover** **over** **links** to see the real URL before clicking.7

### Q5: What is Secure Sockets Layer (SSL), and why is it important?

**Answer:** SSL is a **security** **protocol** that encrypts data during online transactions.

* + Used for **banking,** **shopping,** **emails,** **and** **messaging**.
  + Ensures **data** **is** **secure** **and** **private**.
  + Prevents **data** **interception** **(man-in-the-middle** **attacks)**.

Websites using SSL have **a** **padlock** **symbol** **and** **‘https://’ in** **the** **URL**.

## Write your Answers on your Notebook and Verify it on Next Screen

**Q6:** **How** **does** **multi-factor** **authentication** **(MFA)** **improve** **security?**

**Q7:** **Why** **is** **it** **important** **to** **use** **strong** **passwords,** **and** **how** **can** **users** **manage** **them** **effectively?**

**Q8:** **How** **do** **proxy** **servers** **help** **protect** **users** **online?**

**Q9:** **What** **are** **the** **benefits** **of** **using** **biometric** **authentication** **for** **security?**

**Q10:** **How** **do** **privacy** **settings** **help** **protect** **personal** **information** **online?**

1. **Answer:** MFA adds an extra layer of security by requiring multiple verification factors:
   * **Something** **you** **know** (e.g., password, PIN).
   * **Something** **you** **have** (e.g., security token, mobile device).
   * **Something** **you** **are** (e.g., fingerprint, facial recognition).

**Benefit:** Even if a hacker steals a password, they cannot access an account without the additional authentication factor.

1. **Answer:** Weak passwords can be easily guessed or cracked, leading to unauthorized access.

### Best Practices:

* + Use complex passwords with uppercase, lowercase, numbers, and symbols.
  + Avoid using personal information like birthdates or names.
  + Use a password manager to securely store and generate strong passwords.

1. **Answer:** Proxy servers act as intermediaries between users and the internet. They:
   * Hide IP addresses for anonymity.
   * Block access to harmful or restricted websites.
   * Filter and inspect traffic to prevent cyber threats.
   * Improve performance by caching frequently visited web pages.
2. **Answer:** Biometric authentication improves security by using unique physical traits that are difficult to duplicate.

### Examples:

* + **Fingerprint** **scanners** (used in smartphones and laptops).
  + **Facial** **recognition** (used for secure logins).
  + **Retina** **scans** (used in high-security environments).

**Advantage:** Unlike passwords, biometric data cannot be easily stolen or guessed.

1. **Answer:** Privacy settings control what data is shared and who can access it.

### Key Features:

* + "Do Not Track" settings limit website tracking.
  + Managing cookie settings prevents excessive data collection.
  + Restricting profile visibility protects personal information on social media.
  + Reviewing saved payment methods reduces financial risks.