**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.

**2. 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** | Saves usernames, passwords, and email addresses for easier future logins. |
| **Personalized experience** | Recognizes users and applies saved preferences (e.g., dark mode, preferred language). |
| **Shopping cart memory** | Saves items in an online shopping cart, even after the browser is closed. |
| **Tracking internet habits** | 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** | Stores game progress and settings. |
| **Social media preferences** | 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:

1. **Remember login details and preferences**.
2. **Store shopping cart items**.
3. **Track user activity** for personalized recommendations.
4. **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?**

**6. Answer:**

1. **First-party cookies** → Created by the website the user is visiting; used for login details, preferences, and user experience.
2. **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.
3. 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).

**7. 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.
3. Example: In Google Chrome → Settings > Privacy and Security > Cookies and other site data.

**8. 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.
3. **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.

**9. 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.

**10. 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.