COOKIES: A CONCEPTUAL STUDY

Ms. Shagundeep Kaur*

Introduction:

Cookies are tiny text files that are maintained in the data folder or browser directory of an online user. They are sometimes referred to as browser cookies or HTTP cookies. Cookies are stored on users' browsers by e-commerce websites in order to remember login information, identify visitors, and provide a customized shopping experience. HTTP cookies are little data packets that a web server generates while a user is viewing a website and that the user's web browser stores on the user's computer or other devices. Web cookies, Internet cookies, browser cookies, and plain old cookies are other names for HTTP cookies. Throughout a session, a website may place a large number of cookies on a user's computer. On the device being used to view the website, cookies are stored.

Cookies are valuable and occasionally necessary tools for the internet. They enable web servers to keep tabs on a user's browsing activities (such as when they click particular buttons, sign in, or note which pages were visited in the user's browser history) or preserve stateful data (such items added to the shopping cart in an online store) on the user's device. They can also be used to save information that users have already entered into form fields, such as names, addresses, passwords, and payment card numbers, for later use.

Cookies used for authentication are regularly used by web servers to confirm which account a user is currently logged in with. Without the cookie, users would need to verify their identity each time they wanted to access a page with sensitive information by checking in. The user's web browser, and whether the cookie data is encrypted are often factors in acookie's security. Due to security weaknesses, a cookie's data may be read by an attacker, used to access user data, or exploited in other ways.

Tracking cookies, especially third-party tracking cookies, are frequently used to compile long-term records of people's browsing activity; this possible privacy issue drove European and American legislators to take action in 2011.European legislation mandates that before installing third-party cookies on users' devices, websites that are intended for the European Union's member states must first get "informed consent" from those users.

Literature Review

According to Lockett (2018), small retail store owners must hire the right employees, implement effective advertising methods, and carefully choose explicit web content to improve sales generated via digital marketing. Leaders of the organization also actively engaged the community to boost sustainability, brand recognition, and growth. In order to produce and advertise products and services for the retail sector as well as to improve the productivity of their businesses, business leaders employ a variety of communication channels.

Assistant Professor; Guru Gobind Singh College for Women, Sector 26, Chandigarh; Email ID: shagundeep@ggscw.ac.in

Cant & Wiid, (2016) claim that social media is a medium for communication. Small business owners can now incorporate online communication into their business plans and use it as a platform for advertising thanks to the Internet phenomenon known as "digital marketing."

Ibrahim et al. (2018) claims that a shift in consumer purchasing behaviors is what makes digital marketers interested in social media advertising. According to social media polls, the average user spends 37 minutes a day on well-known social media platforms like Facebook and Twitter, and 10% of internet users use social media websites. Consider the potential growth in market share that social media marketing could bring to online businesses.

The study (Guru, 2013) stresses how important it is for merchants to gain customers' trust in an online world where transactions are frequently impersonal and anonymous. Compared to conventional marketing strategies, digital technology enables more tailored goods, services, and marketing messages. With the help of these digital tools, marketers are better equipped to respond to changing consumer demands more rapidly and efficiently, building and maintaining positive customer relationships on a much wider scale.

How cookies function

Secure websites employ cookies to authenticate a user's identity as they move between pages; otherwise, each time an item is put into the cart or wish list, login information must be given.

•Customer log-ins, persistent shopping carts, wish lists, and product suggestions are all made possible and improved by cookies.

• Custom user interfaces

• Preserving customer contact and payment information

Session cookies and persistent cookies are the two main types of cookies, and each contains a large number of subgroups.

Session Cookie

A session cookie, also known as an "in-memory cookie," "transient cookie," or "non-persistent cookie," is only used while a user is browsing a website. Session cookies either expire or are deleted when a web browser is closed because session cookies don't have a set expiration date, the browser may identify them. Data is stored in session cookies on the browser until it is closed. Every time a new browser window is launched, the same user is treated as a new visitor and is prompted for their login details.

Persistent cookie

Until that time has elapsed or the cookie is manually deleted, persistent cookies are kept in a browser for a specified period of time. Website visitors can be remembered even after their browsers have closed because of persistent cookies. Persistent cookies provide features like persistent shopping carts, which keep things added to the basket between sessions. A persistent cookie has a predetermined lifespan or expiration date. Information from the

persistent cookie is delivered to the server for the time frame defined by its creator each time a user reaches the website to which it belongs or reads a resource from that website from another website (such as an advertisement). Persistent cookies, sometimes known as tracking cookies, enable advertisers to monitor a user's internet browsing activity over an extended period of time. Additionally, by keeping users logged into their accounts, persistent cookies save users from having to enter their login details each time they visit a page.

Secure cookie

A secure cookie can only be sent over a secure connection (i.e. https). They cannot be transmitted through insecure networks (i.e. http). This lessens the chance of cookie theft by eavesdropping. A cookie can be made secure by including the Secure flag.

Supercookie

A super cookie is a cookie whose origin is a top-level domain (such as.com) or a public suffix (such as .co.uk). On the other hand, common cookies have a specific domain name as their source, such as cookies.com. Super cookies can be a security risk, hence web browsers typically block them. If the browser were to stop filtering cookies, an attacker in charge of a malicious website might create a supercookie that might spoof or obstruct legitimate user requests to websites that share the same top-level domain or public suffix as the malicious website. For instance, a super cookie with the origin of.com could negatively affect a request submitted to cookie.com even though the cookie itself did not originate from cookie.com.

This can be used to change user data or make phoney logins. Using the Public Suffix List lowers the risk that supercookies pose. The Public Suffix List is a cross-vendor initiative that aims to provide a precise and up-to-date list of domain name suffixes. The lack of an updated list in older browser versions may make them vulnerable to supercookies from specific websites.

Zombie cookie

A zombie cookie is a data and code that a web server keeps secretly beyond the visitor's web browser's designated cookie storage place on the visitor's computer or another device. The zombie cookie automatically produces a regular cookie once the original HTTP cookie has been destroyed. The zombie cookie can be kept in a variety of locations, including HTML5 Web storage, Flash Local shared objects, and other client-side and even server-side locations. The JavaScript code will reconstruct the zombie cookie if it is missing from one of these locations using the data from the other locations.

Third party Cookies

Cookies may have a big impact on how anonymous and private web users are. Cookies are only communicated to the server establishing them or another server in the same Internet domain, despite the fact that a web page may contain images or other elements saved on servers in other domains. When these components are retrieved, third-party cookies are

created. A cookie from a domain other than the one that is shown in the address bar is referred to as a third-party cookie. This type of cookie is typically used when web pages include content from other websites, such as banner adverts. This opens the door to tracking a user's browsing history, which advertisers utilize to serve each user with relevant ads.

Website's cookie wall

The cookie wall of a website emerges and informs the user of cookie usage. The website cannot be visited without tracking cookies, and there is no way to reject them.

Digital marketing and cookies

Consider yourself perusing the aisles of a grocery store. The staff members at the shop are aware of your past purchases because you frequent the location occasionally. To encourage you to return and make additional purchases, the store will present you with special deals and combo packs the next time you visit.

Cookies help digital marketers in this way. In this illustration, the store is a website, and the staff members that reported the customer's purchasing behavior are cookies. Digitalmarketersmay improve user experience and increase lead generation by using cookies to learn more about the visitors to their websites.

An e-commerce website keeps a record of user behavior when a user first visits it on a remote server and a cookie is stored in the user's browser when they visit an e-commerce website for the first time, and the website records their behavior on a remote server. One brief line of text makes up the cookie. It doesn't have any data on the user or their computer. In its place, it usually includes the website's URL, a randomly generated number, and the cookie's expiration date.

When a user navigates to a new page on a website, the browser is prompted to check for cookies. If the cookie's URL matches the website's URL, the website uses the unique generated number to retrieve the user information from its server.

Pros of using cookies in digital marketing

- **Personalization**

  Cookies can retain user information to ensure that they only ever see content that is pertinent to them. For instance, a web server may send a cookie containing the username that was most recently used to log in to a website, enabling it to be filled up automatically the next time the user checks in. Numerous websites utilize cookies to customizethe content according to user choices. Before being submitted to the server, the selections made by users are entered into a web form. The server then sends a cookie with preferences to the browser. By doing this, the server will be able to adapt a page on the website each time a user visits it in accordance with their preferences.

- **Ad Impression Metrics**

Every digital marketer must start with advertising. It is one of the tactics that a digital marketer prioritises the most. These days, advertisements are so pervasive in our lives that everyone is aware of them. People will click on an advertisement if it piques their curiosity or is relevant to a current demand.Because cookies are used to track user behaviour and deliver relevant adverts based on their preferences, this is the case. Every marketer needs to be aware of how effective their advertisements are. Measuring them is the only way they can make their advertisements better.

Cookies support digital marketers in measuring click and impression accuracy. An impression is the total number of times people saw your advertisement, and click accuracy is the total number of times users clicked it. With the help of these statistics, marketers may determine what works and what doesn't in order to produce better commercials.

- **Personalized Ads**

The solution was to offer a customised shopping experience. An advertisement must be pertinent to the specific viewer in order to be effective. A 42-year-old, for instance, will not respond to the same advertisements as a 20-year-old. Advertisements must be placed that appeal to the target market.Cookies can gather the essential data, such as age, gender, location, interests, etc. for the marketerto put advertisements. Over time, this will enhance both the user experience and marketing outcomes.

- **Retargeting Techniques**

Ad retargeting is a technique used by businesses to display advertisements to people who have previously expressed interest in their products. The most common application of this promotion strategy is in digital marketing.

You may have already spotted these commercials; for instance, if you searched for and purchased a watch on Amazon, you may have noticed advertisements for watches all over the place. This is so that Amazon's marketing platform will know that you need a watch after you add one to your cart. As a result, it will display watches and watch offers on other websites you visit.

Digital marketers utilize ad retargeting to increase the conversion rate of site visitors at the point of sale. A digital marketer can accomplish this because of cookies. To get the data required to follow users and provide adverts relevant to their preferences, they employ third-party cookies.

- **Enhances Consumer Engagement**

Virtually every website has numerous pages. When a page is interesting enough, the user stays longer on it. Otherwise, there will be a lot of bounces. It is the duty of the marketer to make the page interesting for the visitors.

Marketers may learn via cookies how long visitors stay on each page and how they engage with it. If visitors are leaving a page quickly, it needs to be optimized to increase engagement.

Conclusion

Digital marketing has taken the role of conventional marketing and communication techniques. Social, cultural, religious, technological, and economic issues all have an impact on the shortage of digital marketing skills. Today, internet advertising is commonplace. Here, how businesses view their clients becomes crucial. 93% of marketers utilize social media for business, which is astounding. In 2022, it was expected that about 92% of American marketers who work for companies with more than 100 employees will startusing social media for marketing. Between 2021 and 2022, there was more than a 10% increase in social media users. In sum, this adds up to more than 376 million more users, giving social media a 4.62 billion-person global reach. As a result, cookies are crucial. Online marketing is the practice of using the internet for advertising. Digital marketing offers marketing channels by using digital technologies. A company's ability to succeed online hinges on its online presence. In order to satisfy customer needs while utilizing digital marketing channels, an integrated strategy is required. To enter this new market successfully, businesses must first understand the way of life of their clients, which can be done with ease when cookies are used.

References

[1] A. Barth. RFC 6265: HTTP State Management System, April 2011.

[2] K. Borders and A. Prakash. Towards Quantification of Network-based Information Leaks via HTTP. In In Proceedings of the Third USENIX Workshop on Hot Topics in Security (HotSEC), San Jose, CA, May 2008.

[3] The Cookie Collective. How We Classify Cookies, 2013. http://cookiepedia.co.uk/classify-cookies.

[4] US Federal Trade Commission. Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers, December 2010.

[5] Italo Dacosta, Saurabh Chakradeo, Mustaque Ahamad, and Patrick Traynor. One-time Cookies: Preventing Session Hijacking Attacks with Stateless Authentication Tokens. ACM Transactions on Internet Technololgy, 12(1):1:1–1:24, July 2012. [6] Steven Englehardt, Dillon Reisman, Christian Eubank, Peter Zimmerman, Jonathan Mayer, Arvind Narayanan, and Edward W Felten. Cookies that give you away: The surveillance implications of web tracking. In Proceedings of the 24th International Conference on World Wide Web, pages 289–299. International World Wide Web Conferences Steering Committee, 2015.

[7] Zachary Evans and Hossain Shahriar. Web session security: Attack and defense techniques. Case Studies in Secure Computing: Achievements and Trends, page 389, 2014.

[8] Kevin Fu, Emil Sit, Kendra Smith, and Nick Feamster. Dos and Don'Ts of Client Authentication on the Web. In Proceedings of the 10th Conference on USENIX Security Symposium - Volume 10, SSYM'01, pages 19–19, Berkeley, CA, USA, 2001. USENIX Association.

[9] John Giannandrea and Lou Montulli. Persistent Client State: HTTP Cookies, October 1994.

[10] Arthur Goldberg, Robert Buff, and Andrew Schmitt. A comparison of HTTP and HTTPS performance. Computer Measurement Group, CMG98, 1998.

[11] Ghostery Inc. Ghostery, 2014.

[12] JISC Legal Information. EU Cookie Directive - Directive 2009/136/EC, April 2010.

[13] Martin Johns. SessionSafe: Implementing XSS Immune Session Handling. In Dieter Gollmann, Jan Meier, and Andrei Sabelfeld, editors, Computer Security - ESORICS 2006, volume 4189 of Lecture Notes in Computer Science, pages 444–460. Springer Berlin Heidelberg, 2006.

[14] B. Krishnamurthy, D. Malandrino, and C. Wills. Measuring Privacy Loss and the Impact of Privacy Protection in Web Browsing. In In Proceedings of the Symposium on Usable Privacy and Security, Pittsburgh, PA, July 2007.

[15] B. Krishnamurthy and C. Wills. Generating a Privacy Footprint on the Internet. In In Proceedings of the ACM Internet Measurement Conference, Rio de Janerio, Brazil, October 2006.

[16] B. Krishnamurthy and C. Wills. Characterizing Privacy in Online Social Networks. In In Proceedings of the ACM SIGCOMM Workshop on Online Social Networks, Seattle, WA, August 2008.