What is Browser Fingerprinting?

Privacy in the modern world is the biggest myth. Cybercriminals, marketers, ad agencies, and other use numerous ways to infiltrate your privacy and gain your information. One of the common ways is Browser Fingerprinting.

In this post, we would discuss what Browser Fingerprinting is, how it works, why browser fingerprinting is used, and how to prevent it from happening.

What is Browser Fingerprinting?

Browser Fingerprinting is the modern tracking technique that websites use for collecting prominent information about users, such as search history, time zone, default language, and many more. Almost every latest website uses scripts to function properly. Scripts contain a set of information to direct the website on what function to perform. Since Scripts execute in the background, users would know about it working. Advertisers, marketers, and others take this as an advantage and create a special Script that can collect all your information while you are browsing the internet. Since every user browses the internet differently, the data collected would be unique, like fingerprints.

Most people might confuse Browser Fingerprinting with Cookies. However, both of them are different. While Cookies are regulated, i.e., websites need to take user permission before using the Cookies, there are no such restrictions for Browser Fingerprinting. The users can easily delete Cookies, while an average internet user cannot even trace the Browser Fingerprinting.

How does Browser Fingerprinting work?

As already mentioned, Browser Fingerprinting works by collecting unique user data through specially designed Scripts. Generally, Scripts play a vital role in running the website by conducting functions like video rendering, running web applications, optimizing web pages' loading time, and more. The website developers can use advanced APIs to fetch user information using scripts. The danger is, there is no way to distinguish a Browser Fingerprinting Script from any other Script as all functions the same.

After the Browsing Fingerprint Script is loaded, it can collect various data from the device such as installed OS, installed applications, time zone, browsing data, browsing settings, shopping preference, plugins used, and more such data which can be converted into a hash or a digital fingerprint.

What is the purpose of Browser Fingerprinting?

Till now, it might be clear that the primary purpose of Browser Fingerprinting is web tracking and collecting confidential data for ad targeting. The organization claims to track your data for providing you optimized and personalized web experience. However, the amount and the type of data collected in the name of delivering a better web experience is immense and can be used for many other purposes. For example, the data collector can sell the data to cybercriminals on the dark web in return for a good amount of money. The data can also be provided to government agencies for tracking any user without its consent.

Since everything you search on the internet is collected through Browser Fingerprinting, the data collectors might even know very intimate details about you and blackmail you with that. The data collection can also lead to an increase in air travel fares and insurance prices.

How to prevent Browser Fingerprinting?

To be honest, there is no solid way to prevent Browser Fingerprinting from happening to you. It is because many legitimate websites use it to collect your data in the name of providing better services. Even using the Incognito Mode or VPN cannot prevent Browser Fingerprinting. You might think that shutting the Web Scripts can do the trick and stop it, but most modern websites cannot run without enabling the Scripts, so disabling them is not a feasible option. However, there are still some ways to limit Browser Fingerprinting. **For example −**

- Web Plugins such as Privacy Badger can detect and prevent the tracking and spying web scripts from loading. Keep them installed on your browser.
- Some anti-track plugins and extensions can prevent Browser Fingerprinting by Generalization and Randomization. Generalization means manipulating the browser API result so that there is no uniqueness found in your browsing print. Randomization means changing your web attributes periodically and randomly so that there is no pattern to identify.
- There are privacy-focused browsers such as Tor that block every type of trackers on its platform. So if you are pretty concerned about your privacy, use such web browsers for browsing the internet.