РУССКИЙ

1. Файлы cookie - это текстовые файлы с небольшими фрагментами данных.
2. Файлы cookie HTTP созданы для веб-браузеров, чтобы отслеживать, персонализировать и сохранять информацию о сеансе каждого пользователя.
3. «Сеанс» просто означает время, которое вы проводите на сайте.
4. Файлы cookie создаются для вашей идентификации при посещении нового веб-сайта.
5. Сервер отправляет короткий поток идентифицирующей информации в ваш браузер.
6. Файлы cookie браузера идентифицируются и считываются парами «имя-значение».
7. Они сообщают cookie-файлам, куда следует отправлять и какие данные следует вспомнить.
8. Сервер отправляет файл cookie тогда, когда он хочет, чтобы браузер сохранил его.
9. Ваш браузер сохранит файлы cookie локально, чтобы запомнить «пару имя-значение», которая идентифицирует вас.
10. Если пользователь вернется на этот сайт в будущем, браузер вернет эти данные на сервер в виде файла cookie.
11. Это когда ваш браузер отправит его обратно на сервер, чтобы восстановить данные из ваших предыдущих сеансов.
12. Веб-сайты используют файлы cookie HTTP для оптимизации вашего веб-опыта.
13. Без файлов cookie вам придется снова войти в систему после того, как вы покинете сайт.
14. HTTP-файлы cookie необходимы для современного Интернета, но представляют собой уязвимость для вашей конфиденциальности.
15. Хотя большинство файлов cookie совершенно безопасны, некоторые из них могут использоваться для отслеживания вас без вашего согласия.
16. Они не могут заразить компьютеры вирусами или другим вредоносным ПО.
17. Однако некоторые кибератаки могут захватить файлы cookie и предоставить доступ к вашим сеансам просмотра.
18. Опасность заключается в их способности отслеживать истории просмотров отдельных пользователей.
19. Независимо от того, как вы обрабатываете файлы cookie, лучше всего оставаться начеку и часто очищать файлы cookie.

АНГЛИЙСКИЙ

1. Cookies are text files with small pieces of data.
2. HTTP cookies are built for Internet web browsers to track, personalize, and save information about each user’s session.
3. A “session” just refers to the time you spend on a site.
4. Cookies are created to identify you when you visit a new website.
5. The server sends a short stream of identifying info to your browser.
6. Browser cookies are identified and read by “name-value” pairs.
7. These tell cookies where to be sent and what data to recall.
8. The server sends the cookie when it wants the browser to save it.
9. Your browser will store it locally to remember the “name-value pair” that identifies you.
10. If a user returns to that site in the future, the browser returns that data to the web server in the form of a cookie.
11. This is when your browser will send it back to the server to recall data from your previous sessions.
12. Websites use HTTP cookies to streamline your web experiences.
13. Without cookies, you’d have to login again after you leave a site.
14. HTTP cookies are essential to the modern Internet but a risk to your privacy.
15. While most cookies are perfectly safe, some can be used to track you without your consent.
16. They can't infect computers with viruses or other malware.
17. However, some cyberattacks can hijack cookies and enable access to your browsing sessions.
18. The danger lies in their ability to track individuals' browsing histories.
19. Regardless of how you handle cookies, it’s best to remain on guard and clean up your cookies often.