ФЕДЕРАЛЬНЫЙ ЭКОЛОГИЧЕСКИЙ ОПЕРАТОР РОСАТОМ

ПОВЫШЕНИЕ ОСВЕДОМЛЕННОСТИ

УЯЗВИМЫЕ ВЕРСИИ БРАУЗЕРОВ

Федеральная государственная информационная система учета и контроля за обращением с отходами I и II классов опасности.
Федеральный оператор по обращению с отходами I и II классов опасности.

Основные угрозы при использовании уязвимых версий популярных браузеров

Эксплойты и удалённое управление

Хакеры могут использовать уязвимости старого браузера для выполнения вредоносного кода на вашем устройстве. Это может привести к заражению вирусами, краже личных данных или даже удалённому управлению компьютером. В худшем случае злоумышленник получит полный контроль над системой, включая файлы, веб-камеру и микрофон.

Фишинг и кража данных

Без актуальных механизмов безопасности браузер может не распознать поддельные сайты, которые маскируются под настоящие. Вы можете ввести логин и пароль на поддельном сайте, думая, что заходите в онлайн-банк или почту. Как только данные окажутся в руках мошенников, они смогут украсть деньги или использовать ваш аккаунт в своих целях.

Отслеживание без вашего ведома

Уязвимости в браузере могут позволять сайтам и рекламным трекерам следить за вами, даже если включены настройки конфиденциальности. Это может привести к сбору информации о ваших привычках, местоположении и даже к целенаправленным атакам. В результате вы рискуете стать жертвой персонализированных фишинговых атак, когда мошенники используют собранные о вас данные.

Утечка личной информации

Уязвимости в браузере позволяют злоумышленникам похищать ваши пароли, файлы, историю посещений и даже банковские данные. Некоторые атаки позволяют перехватывать вводимые на сайтах данные, включая переписку в мессенджерах. Это особенно опасно, если вы используете один и тот же пароль для разных сервисов — взломав один аккаунт, хакеры могут получить доступ ко всем остальным.

Атаки «человек посередине» (MITM)

Устаревший браузер может не проверять подлинность сертификатов сайтов, что делает вас уязвимым для перехвата трафика. Злоумышленник может подменить страницу, на которую вы заходите, и внедрить в неё вредоносный код. В результате ваши пароли, номера карт и другие конфиденциальные данные окажутся у хакеров.

Вредоносные расширения

В старых версиях браузеров могут существовать уязвимости, позволяющие устанавливать вредоносные расширения без ведома пользователя. Такие плагины могут красть личные данные, показывать навязчивую рекламу или перенаправлять вас на фишинговые сайты. Некоторые из них даже получают доступ к веб-камере и микрофону, что угрожает вашей приватности.

Как себя обезопасить?

Всегда обновляйте браузер до последней версии

📌 Производители браузеров регулярно выпускают обновления, закрывающие уязвимости и повышающие безопасность.

📌 Если браузер не обновляется автоматически, проверяйте наличие новых версий вручную в настройках.

📌 Использование устаревшего ПО значительно увеличивает риск заражения вирусами и кражи данных.

Антивирусное ПО и используйте брандмауэр

🛡️ Надёжный антивирус поможет обнаружить вредоносные сайты, защитит от троянов и фишинговых атак.

🛡️ Брандмауэр блокирует подозрительные подключения, предотвращая несанкционированный доступ к вашему устройству.

🛡️ Регулярное сканирование системы поможет выявить угрозы, которые могли попасть на компьютер через браузер.

Проверяйте адреса сайтов

🔍 Фишинговые сайты часто имитируют известные ресурсы, но имеют поддельные URL-адреса.

🔍 Всегда проверяйте, что сайт использует HTTPS и его домен написан без ошибок.

🔍 Никогда не переходите по подозрительным ссылкам из писем, сообщений в мессенджерах и соцсетях.