Ни один злоумышленник больше не сможет воспользоваться вашими данными в злонамеренных целях.

LastPass — это компания, которая разрабатывает и предоставляет одноимённый сервис для хранения паролей. Сервис помогает генерировать и хранить сложные пароли, а также автоматически заполнять их на веб-сайтах.
 LastPass также предоставляет доступ к паролям с любого устройства с помощью онлайн-синхронизации. Сервис обеспечивает дополнительные опции, такие как шифрование и общий доступ к паролям." data-html="true" data-original-title="LastPass" >LastPass, популярный менеджер паролей, объявил о скором начале шифрования URL («Uniform Resource Locator» или «Единый Указатель Ресурсов») — единый для всех сайтов определитель места положения ресурса в сети Интернет. URL делится на составные части: домен, путь к странице и имя файла.

 Изначально URL был изобретен для обозначения местоположения различных файлов в Интернете, и только со временем стал использоваться для того, чтобы обозначать адреса всех ресурсов, независимо от их типа." data-html="true" data-original-title="URL" >URL-адресов, хранящихся в пользовательских хранилищах. Этот шаг направлен на усиление конфиденциальности данных и защиту от утечек и несанкционированного доступа.

Внедрение новой функции станет значительным шагом в направлении реализации архитектуры нулевого разглашения, что означает, что даже сам LastPass не будет иметь никакого доступа к данным пользователей. Шифрование URL-адресов будет происходить автоматически и незаметно благодаря возросшей производительности современного оборудования.

Исторически сложилось так, что в 2008 году, из-за ограничений вычислительной мощности, инженеры LastPass приняли решение не шифровать URL-адреса, чтобы снизить нагрузку на процессоры и минимизировать энергопотребление. С развитием технологий эти ограничения больше не актуальны, и теперь компания может шифровать и расшифровывать URL-адреса без заметных задержек в работе своего продукта.

Шифрование URL-адресов необходимо для повышения безопасности пользователей и соответствия архитектуре нулевого разглашения. В URL-адресах могут содержаться детали о природе учётных записей, таких как банковские, почтовые или социальные сети. Шифрование этих данных поможет сохранить их конфиденциальность и снизить риски.

В 2022 году LastPass столкнулся с двумя утечками данных, в результате которых

злоумышленники получили доступ к исходному коду, данным пользователей и резервным копиям, включая зашифрованные хранилища паролей. Несмотря на то, что для расшифровки этих хранилищ требовался мастер-пароль, утечки включали незашифрованные URL-адреса, что позволило злоумышленникам целенаправленно атаковать учётные записи в финансовых сервисах.

Некоторые слабые мастер-пароли были расшифрованы, и с их помощью были взломаны криптовалютные биржи, что привело к хищению более $4 миллионов. Это дополнительно подтверждает тот факт, что шифрования много не бывает, и, при наличии такой возможности, им нужно защитить все данные, хранящиеся в таких чувствительных сервисах, как, например, LastPass.

Внедрение шифрования URL-адресов в LastPass потребует переработки клиентских и серверных компонентов. Первая фаза реализации начнётся в июне 2024 года и будет включать автоматическое шифрование основных полей URL для всех существующих и новых учётных записей. В это время будут удалены дублирующие и устаревшие поля URL, а пользователи получат уведомления о внесённых изменениях.

Вторая фаза шифрования запланирована на вторую половину года и будет охватывать оставшиеся шесть полей URL, включая эквивалентные домены, подстановочные URL, перенаправляющие URL, пользовательские URL, URL в заметках и исторические URL.

Пользователям не нужно предпринимать никаких действий, так как LastPass автоматически отправит все инструкции по использованию новых функций, когда процесс развёртывания перейдёт в активную фазу.