Риски для приватности в приложениях-сканерах QR-кодов и как их избежать

Большинство бесплатных сканеров QR-кодов отслеживают каждое ваше сканирование. Узнайте, какие данные они собирают и как защититься по-настоящему приватным сканером.

Автор: Lubor Šimůnek · Опубликовано: August 9, 2026 · Продуктивность

Онлайн-версия: https://appstoryo.com/ru/blog/qr-code-scanner-privacy-no-tracking



Ваш сканер QR-кодов может знать о вас больше, чем вы думаете

Когда вы скачиваете бесплатный сканер QR-кодов из магазина приложений, вы, скорее всего, думаете об удобстве. О приватности вы вспоминаете в последнюю очередь. А стоило бы — в первую.

За последние несколько лет исследователи безопасности и защитники приватности неоднократно обнаруживали, что популярные бесплатные сканеры QR-кодов используют агрессивные методы сбора данных, которых большинство пользователей просто не замечает. В этой статье подробно разбирается, какие именно данные собирают такие приложения, как они их используют и что вы можете сделать для собственной защиты.

Какие данные на самом деле собирают приложения-сканеры QR-кодов?

Ответ зависит от конкретного приложения, но чаще всего сканеры QR-кодов, живущие за счёт рекламы, собирают следующее:

1. QR-коды, которые вы сканируете

Это самые чувствительные данные и одновременно те, о которых забывают чаще всего. Многие сканеры QR-кодов записывают каждый отсканированный код и передают расшифрованное содержимое на удалённые серверы. В этом содержимом могут быть пароли от Wi-Fi (закодированные в формате QR), приватные ссылки на переговорные комнаты, коды подтверждения записи к врачу, внутренние корпоративные ссылки или банковские платёжные QR-коды.

Когда вы сканируете QR-код в кабинете врача и эта ссылка незаметно уходит на аналитический сервер, вы невольно раскрываете информацию о своём здоровье. Когда вы сканируете платёжный QR-код и эти данные записываются в журнал, это раскрытие финансовой информации.

2. Ваше местоположение

Многие сканеры QR-кодов запрашивают доступ к точному GPS-местоположению. Формально это делается, чтобы «улучшить пользовательский опыт», но на практике служит для построения геоповеденческого профиля: куда вы ходите, когда сканируете там QR-коды и какие типы кодов встречаются вам в разных местах.

3. Идентификаторы устройства

Даже без доступа к геолокации приложения могут составить цифровой отпечаток вашего устройства, объединив модель, разрешение экрана, версию ОС, список установленных приложений и рекламный идентификатор. Такой отпечаток остаётся неизменным даже после переустановки приложения и позволяет отслеживать вас в разных сервисах.

4. Поведенческая аналитика

Большинство популярных сканеров QR-кодов встраивают сторонние аналитические SDK — чаще всего Firebase Analytics, Mixpanel, Amplitude, Adjust или AppsFlyer. Эти SDK фиксируют, как часто вы открываете приложение, какими функциями пользуетесь, сколько длится каждая сессия и как вы взаимодействуете с рекламой.

5. Доступ к контактам и хранилищу

Некоторые сканеры запрашивают доступ к вашим контактам и памяти устройства. Доступ к списку контактов позволяет приложениям сопоставить вашу личность с номерами телефонов и адресами электронной почты в базах рекламодателей, что резко повышает ценность вашего профиля.

Проблема отслеживающих пикселей

Некоторые сканеры QR-кодов идут ещё дальше и встраивают отслеживающие пиксели в веб-представления, в которых показывают отсканированные ссылки. Когда вы сканируете QR-код и приложение открывает страницу во встроенном браузере, оно может читать файлы cookie, внедрять JavaScript и отслеживать ваше поведение на целевом сайте — полностью без вашего ведома.

Реальные примеры проблем с приватностью в сканерах QR-кодов

В 2020 году широко используемый сканер QR-кодов был удалён из Google Play Store после того, как исследователи обнаружили в нём вредоносный код, перехватывавший трафик браузера. В 2021 году специалисты по приватности выяснили, что несколько ведущих сканеров QR-кодов отправляли данные отсканированных ссылок на серверы в юрисдикциях со слабым законодательством о защите данных. В 2022 году выяснилось, что популярный сканер считывал содержимое буфера обмена пользователя, перехватывая пароли и конфиденциальный текст.

Как выглядит сканер QR-кодов, уважающий приватность

По-настоящему приватный сканер QR-кодов обладает следующими свойствами:

- **Нет разрешения на доступ в интернет** — он никуда не может отправить данные, потому что не способен выполнять сетевые запросы
- **Нет аналитических SDK** — ни Firebase, ни Mixpanel, ни AppsFlyer
- **Нет рекламных сетей** — ни AdMob, ни Meta Audience Network
- **Минимум разрешений** — только камера
- **Обработка на устройстве** — всё декодирование происходит локально, ничего не передаётся
- **Не требуется аккаунт** — нет личности, к которой можно привязать историю сканирований

QR Code Reader Without Ads: приватность заложена в основу

QR Code Reader Without Ads создан именно по этим принципам. У приложения нет разрешения на доступ в интернет — оно буквально не может выполнить сетевой запрос, — а значит, отправка данных ваших сканирований на какой-либо сервер архитектурно невозможна. В нём нет ни рекламных SDK, ни аналитических библиотек, ни отслеживающих пикселей.

Движок распознавания QR-кодов работает целиком на вашем устройстве и опирается на проверенные библиотеки с открытым исходным кодом. Когда вы сканируете QR-код со ссылкой, приложение показывает вам эту ссылку для проверки, прежде чем открыть её в браузере по умолчанию.

Аккаунт не нужен. Экрана регистрации нет. История ваших сканирований остаётся на вашем устройстве.

Готовы перейти на приватный сканер QR-кодов? Скачайте QR Code Reader Without Ads бесплатно:

Скачать в Google Play — бесплатно, без рекламы, без слежки

Также доступно для iPhone и iPad:

Скачать в App Store — бесплатно, без рекламы, без слежки

Как проверить приватность вашего нынешнего сканера QR-кодов

Если вы пока не готовы менять приложение, вот как оценить приватность вашего текущего сканера QR-кодов:

1. **Проверьте разрешения приложения** — откройте Настройки → Приложения → [ваш сканер] → Разрешения. Если у него есть доступ к геолокации, контактам или хранилищу без очевидной функциональной необходимости, это тревожный знак.
2. **Изучите политику конфиденциальности** — ищите формулировки вроде «сторонние партнёры», «рекламные сети» и «передача данных».
3. **Используйте сетевой монитор** — инструменты вроде NetGuard (Android) покажут, с какими доменами связываются ваши приложения.
4. **Загляните в базу Exodus Privacy** — Exodus Privacy анализирует Android-приложения (APK) и перечисляет все трекеры и разрешения в каждом из них.

Главный вывод

QR-коды повсюду — меню в ресторанах, билеты на мероприятия, платёжные терминалы, упаковка товаров и медицинские бланки. Каждый раз, сканируя такой код, вы потенциально раскрываете информацию о том, где вы находитесь и чем занимаетесь. Именно выбранное вами приложение-сканер определяет, останется ли эта информация приватной или будет тихо превращена в деньги.

Сделайте выбор в пользу приватности. Скачайте QR Code Reader Without Ads прямо сейчас:

Установить QR Code Reader Without Ads из Google Play

Установить QR Code Reader Without Ads из App Store

Как цитировать: Lubor Šimůnek (2026). *Риски для приватности в приложениях-сканерах QR-кодов и как их избежать*. AppStoryo, lapnito.cz s.r.o.. https://appstoryo.com/ru/blog/qr-code-scanner-privacy-no-tracking
© 2026 lapnito.cz s.r.o.