Die Datenschutzrisiken von QR-Code-Scanner-Apps – und wie Sie sie vermeiden

Die meisten kostenlosen QR-Scanner verfolgen jeden Ihrer Scans. Erfahren Sie, welche Daten sie sammeln und wie Sie sich mit einem wirklich privaten Scanner schützen.

Autor: Lubor Šimůnek · Veröffentlicht: August 9, 2026 · Produktivität
Online-Version: https://appstoryo.com/de/blog/qr-code-scanner-privacy-no-tracking



Ihr QR-Scanner weiß womöglich mehr über Sie, als Ihnen lieb ist

Wenn Sie sich einen kostenlosen QR-Code-Scanner aus dem App-Store herunterladen, denken Sie vermutlich vor allem an Bequemlichkeit. Datenschutz ist das Letzte, woran Sie denken. Dabei sollte er an erster Stelle stehen.

In den vergangenen Jahren haben Sicherheitsforscher und Datenschützer immer wieder festgestellt, dass beliebte kostenlose QR-Scanner-Apps aggressive Datensammelpraktiken enthalten, die den meisten Nutzern nie auffallen. Dieser Artikel zeigt genau, welche Daten diese Apps erfassen, wie sie sie verwenden und was Sie zu Ihrem Schutz tun können.

Welche Daten sammeln QR-Scanner-Apps tatsächlich?

Die Antwort hängt von der jeweiligen App ab, doch zu den am häufigsten von werbefinanzierten QR-Scannern erfassten Daten gehören:

1. Die QR-Codes, die Sie scannen

Das ist die sensibelste und zugleich am häufigsten übersehene Datenart. Viele QR-Scanner-Apps protokollieren jeden gescannten Code und übertragen den entschlüsselten Inhalt an entfernte Server. Dieser Inhalt kann WLAN-Passwörter (im QR-Format codiert), private Meetingraum-URLs, Bestätigungscodes für Arzttermine, interne Unternehmenslinks oder Bezahl-QR-Codes von Banken umfassen.

Wenn Sie in einer Arztpraxis einen QR-Code scannen und diese URL unbemerkt an einen Analyse-Server hochgeladen wird, haben Sie unfreiwillig etwas über Ihre Gesundheit preisgegeben. Wenn Sie einen Bezahl-QR-Code scannen und diese Daten protokolliert werden, ist das eine finanzielle Offenlegung.

2. Ihr Standort

Viele QR-Scanner-Apps verlangen Zugriff auf Ihren genauen GPS-Standort. Angeblich dient das dazu, „das Nutzererlebnis zu verbessern", in der Praxis wird daraus jedoch ein geografisches Verhaltensprofil erstellt: wohin Sie gehen, wann Sie dort QR-Codes scannen und welche Arten von Codes Ihnen an welchen Orten begegnen.

3. Gerätekennungen

Selbst ohne Standortzugriff können Apps einen Fingerabdruck Ihres Geräts erstellen – aus Gerätemodell, Bildschirmauflösung, Betriebssystemversion, Liste der installierten Apps und Werbe-ID. Dieser Fingerabdruck bleibt auch nach einer Neuinstallation stabil und lässt sich nutzen, um Sie über mehrere Dienste hinweg zu verfolgen.

4. Verhaltensanalyse

Die meisten populären QR-Scanner binden Analyse-SDKs von Drittanbietern ein – Firebase Analytics, Mixpanel, Amplitude, Adjust oder AppsFlyer sind verbreitet. Diese SDKs erfassen, wie oft Sie die App öffnen, welche Funktionen Sie nutzen, wie lange jede Sitzung dauert und wie Sie mit Werbung interagieren.

5. Zugriff auf Kontakte und Speicher

Manche Scanner-Apps fordern Zugriff auf Ihre Kontakte und Ihren Speicher an. Der Zugriff auf Ihr Adressbuch erlaubt es Apps, Ihre Identität mit Telefonnummern und E-Mail-Adressen in Werbedatenbanken abzugleichen, was den Wert Ihres Profils drastisch erhöht.

Das Problem der Tracking-Pixel

Einige QR-Scanner-Apps gehen noch weiter und betten Tracking-Pixel in die Webansichten ein, mit denen sie gescannte URLs anzeigen. Wenn Sie einen QR-Code scannen und die App das Ziel im integrierten Browser öffnet, kann sie Cookies auslesen, JavaScript einschleusen und Ihr Verhalten auf der Zielwebsite verfolgen – ganz ohne Ihr Wissen.

Reale Beispiele für Datenschutzprobleme bei QR-Scannern

2020 wurde eine weit verbreitete QR-Scanner-App aus dem Google Play Store entfernt, nachdem Forscher entdeckt hatten, dass sie Schadsoftware enthielt, die den Browser-

Datenverkehr abfing. 2021 stellten Datenschutzforscher fest, dass mehrere der beliebtesten QR-Scanner-Apps gescannte URL-Daten an Server in Ländern mit schwachem Datenschutzrecht sendeten. 2022 kam heraus, dass eine populäre Scanner-App den Inhalt der Zwischenablage auslas – und dabei Passwörter und vertrauliche Texte abgriff.

So sieht ein datenschutzfreundlicher QR-Scanner aus

Ein wirklich privater QR-Code-Scanner hat folgende Eigenschaften:

- **Keine Internetberechtigung** – er kann keine Daten irgendwohin senden, weil er keine Netzwerkaufrufe durchführen kann
- **Keine Analyse-SDKs** – kein Firebase, kein Mixpanel, kein AppsFlyer
- **Keine Werbenetzwerke** – kein AdMob, kein Meta Audience Network
- **Minimale Berechtigungen** – ausschließlich die Kamera
- **Verarbeitung auf dem Gerät** – die gesamte Decodierung läuft lokal ab, nichts wird übertragen
- **Kein Konto erforderlich** – es gibt keine Identität, mit der Ihr Scanverlauf verknüpft werden könnte

QR Code Reader Without Ads: von Grund auf für den Datenschutz gebaut

QR Code Reader Without Ads wurde genau nach diesen Grundsätzen entwickelt. Die App besitzt keine Internetberechtigung – sie kann buchstäblich keinen Netzwerkaufruf tätigen –, wodurch es architektonisch unmöglich ist, dass sie Ihre Scandaten an irgendeinen Server sendet. Es gibt keine Werbe-SDKs, keine Analysebibliotheken und keine Tracking-Pixel.

Die QR-Decodierung läuft vollständig auf Ihrem Gerät und stützt sich auf etablierte Open-Source-Bibliotheken. Wenn Sie einen QR-Code mit einer URL scannen, zeigt Ihnen die App die URL zur Prüfung an, bevor sie in Ihrem Standardbrowser geöffnet wird.

Ein Konto ist nicht nötig. Es gibt keinen Registrierungsbildschirm. Ihr Scanverlauf bleibt auf Ihrem Gerät.

Bereit für den Wechsel zu einem privaten QR-Scanner? Laden Sie QR Code Reader Without Ads kostenlos herunter:

Bei Google Play herunterladen – kostenlos, werbefrei, ohne Tracking

Auch für iPhone und iPad verfügbar:

Im App Store herunterladen – kostenlos, werbefrei, ohne Tracking

So prüfen Sie Ihren aktuellen QR-Scanner auf Datenschutz

Falls Sie noch nicht wechseln möchten, können Sie den Datenschutz Ihres aktuellen QR-Scanners so beurteilen:

1. **App-Berechtigungen prüfen** – gehen Sie zu Einstellungen → Apps → [Ihr Scanner] → Berechtigungen. Hat die App ohne klaren funktionalen Grund Zugriff auf Standort,

Kontakte oder Speicher, ist das ein Warnsignal.

2. **Datenschutzerklärung lesen** – suchen Sie nach Begriffen wie „Drittanbieter-Partner", „Werbenetzwerke" und „Datenweitergabe".
3. **Netzwerkmonitor einsetzen** – Werkzeuge wie NetGuard (Android) zeigen Ihnen, mit welchen Domains Ihre Apps kommunizieren.
4. **Exodus-Privacy-Datenbank durchsuchen** – Exodus Privacy analysiert Android-APKs und listet jeden Tracker und jede Berechtigung einer App auf.

Das Fazit

QR-Codes sind überall – Restaurantkarten, Veranstaltungstickets, Bezahlterminals, Produktverpackungen und Formulare beim Arzt. Jedes Mal, wenn Sie einen scannen, geben Sie möglicherweise preis, wo Sie sind und was Sie gerade tun. Die Scanner-App, für die Sie sich entscheiden, bestimmt, ob diese Informationen privat bleiben oder still und leise zu Geld gemacht werden.

Wechseln Sie jetzt. Laden Sie QR Code Reader Without Ads herunter:

QR Code Reader Without Ads bei Google Play holen

QR Code Reader Without Ads im App Store holen

Zitieren als: Lubor Šimůnek (2026). *Die Datenschutzrisiken von QR-Code-Scanner-Apps – und wie Sie sie vermeiden*. AppStoryo, lapnito.cz s.r.o.. https://appstoryo.com/de/blog/qr-code-scanner-privacy-no-tracking
© 2026 lapnito.cz s.r.o.