Los riesgos de privacidad de las apps de escaneo QR y cómo evitarlos

La mayoría de los escáneres QR gratuitos rastrean cada escaneo que haces. Descubre qué datos recogen y cómo protegerte con un escáner realmente privado.

Autor: Lubor Šimůnek · Publicado: August 9, 2026 · Productividad
Versión en línea: https://appstoryo.com/es/blog/qr-code-scanner-privacy-no-tracking



Tu escáner de códigos QR puede saber más sobre ti de lo que imaginas

Cuando descargas un escáner de códigos QR gratuito de la tienda de aplicaciones, probablemente estés pensando en la comodidad. La privacidad es lo último que te pasa por la cabeza. Pero debería ser lo primero.

Durante los últimos años, investigadores de seguridad y defensores de la privacidad han descubierto una y otra vez que las aplicaciones gratuitas de escaneo de códigos QR más populares incorporan prácticas agresivas de recopilación de datos que la mayoría de los usuarios nunca advierte. Este artículo desglosa exactamente qué datos recogen estas aplicaciones, cómo los utilizan y qué puedes hacer para protegerte.

¿Qué datos recopilan realmente las aplicaciones de escaneo QR?

La respuesta varía según la aplicación, pero los datos que con más frecuencia recolectan los escáneres QR financiados con publicidad son estos:

1. Los códigos QR que escaneas

Este es el dato más sensible y, a la vez, el que más se pasa por alto. Muchas aplicaciones de escaneo QR registran cada código que escaneas y transmiten el contenido descodificado a servidores remotos. Ese contenido puede incluir contraseñas de Wi-Fi (codificadas en formato QR), URLs privadas de salas de reuniones, códigos de confirmación de citas médicas, enlaces corporativos internos o códigos QR de pago bancario.

Cuando escaneas un código QR en la consulta de un médico y esa URL se sube de forma silenciosa a un servidor de analítica, has revelado sin querer algo sobre tu salud. Cuando escaneas un código QR de pago y ese dato queda registrado, se trata de una divulgación financiera.

2. Tu ubicación

Muchas aplicaciones de escaneo QR solicitan acceso a tu ubicación GPS precisa. En apariencia esto sirve para «mejorar la experiencia de usuario», pero en la práctica se utiliza para construir un perfil geoconductual: dónde vas, cuándo escaneas códigos QR en esos lugares y qué tipos de códigos encuentras en cada sitio.

3. Identificadores del dispositivo

Incluso sin acceso a la ubicación, las aplicaciones pueden crear una huella digital de tu dispositivo combinando el modelo, la resolución de pantalla, la versión del sistema operativo, la lista de aplicaciones instaladas y el identificador publicitario. Esta huella se mantiene estable aunque reinstales la aplicación y puede usarse para seguirte a través de múltiples servicios.

4. Analítica de comportamiento

La mayoría de los escáneres QR populares integran SDK de analítica de terceros: Firebase Analytics, Mixpanel, Amplitude, Adjust o AppsFlyer son habituales. Estos SDK registran con qué frecuencia abres la aplicación, qué funciones utilizas, cuánto dura cada sesión y cómo interactúas con los anuncios.

5. Acceso a contactos y almacenamiento

Algunas aplicaciones de escaneo piden acceso a tus contactos y a tu almacenamiento. El acceso a la lista de contactos permite a las aplicaciones asociar tu identidad con números de teléfono y direcciones de correo presentes en bases de datos publicitarias, lo que aumenta enormemente el valor de tu perfil.

El problema de los píxeles de seguimiento

Algunas aplicaciones de escaneo QR van todavía más lejos e incrustan píxeles de seguimiento en las vistas web que utilizan para mostrar las URLs escaneadas. Cuando escaneas un código QR y la aplicación abre el destino en su navegador integrado, la aplicación puede leer cookies, inyectar JavaScript y rastrear tu comportamiento en el sitio web de destino, todo ello sin que lo sepas.

Casos reales de problemas de privacidad en escáneres QR

En 2020, una aplicación de escaneo QR muy utilizada fue retirada de Google Play Store después de que los investigadores descubrieran que contenía malware capaz de interceptar el tráfico del navegador. En 2021, investigadores de privacidad detectaron que varias de las principales aplicaciones de escaneo QR enviaban los datos de las URLs escaneadas a servidores situados en jurisdicciones con leyes de protección de datos débiles. En 2022, se descubrió que una aplicación de escaneo popular leía el contenido del portapapeles del usuario, capturando contraseñas y textos confidenciales.

Cómo es un escáner QR que respeta la privacidad

Un escáner de códigos QR realmente privado tiene las siguientes características:

- **Sin permiso de internet**: no puede enviar datos a ninguna parte porque no puede realizar llamadas de red
- **Sin SDK de analítica**: nada de Firebase, ni Mixpanel, ni AppsFlyer
- **Sin redes publicitarias**: nada de AdMob ni Meta Audience Network
- **Permisos mínimos**: solo la cámara
- **Procesamiento en el dispositivo**: toda la descodificación ocurre localmente, no se transmite nada
- **Sin necesidad de cuenta**: no hay ninguna identidad a la que vincular tu historial de escaneos

QR Code Reader Without Ads: creado para la privacidad desde su base

QR Code Reader Without Ads se diseñó exactamente con estos principios. La aplicación no tiene permiso de internet —literalmente no puede realizar una llamada de red—, lo que significa que resulta arquitectónicamente imposible que envíe tus datos de escaneo a ningún servidor. No hay SDK publicitarios, ni bibliotecas de analítica, ni píxeles de seguimiento.

El motor de descodificación QR funciona íntegramente en tu dispositivo mediante bibliotecas de código abierto consolidadas. Cuando escaneas un código QR que contiene una URL, la aplicación te muestra esa URL para que la revises antes de abrirla en tu navegador predeterminado.

No se requiere ninguna cuenta. No hay pantalla de registro. Tu historial de escaneos permanece en tu dispositivo.

¿Listo para cambiar a un escáner QR privado? Descarga QR Code Reader Without Ads gratis:

Descárgalo en Google Play: gratis, sin anuncios, sin rastreo

También disponible para iPhone y iPad:

Descárgalo en la App Store: gratis, sin anuncios, sin rastreo

Cómo auditar la privacidad de tu escáner QR actual

Si todavía no quieres cambiar de aplicación, así puedes evaluar la privacidad de tu escáner QR actual:

1. **Revisa los permisos de la aplicación**: ve a Ajustes → Aplicaciones → [tu escáner] → Permisos. Si tiene acceso a Ubicación, Contactos o Almacenamiento sin una razón funcional clara, es una señal de alarma.
2. **Lee la política de privacidad**: busca expresiones como «socios externos», «redes publicitarias» y «compartir datos».
3. **Usa un monitor de red**: herramientas como NetGuard (Android) te muestran con qué dominios se comunican tus aplicaciones.
4. **Consulta la base de datos de Exodus Privacy**: Exodus Privacy analiza los APK de Android y enumera todos los rastreadores y permisos de cada aplicación.

En resumen

Los códigos QR están en todas partes: cartas de restaurante, entradas de eventos, terminales de pago, envases de productos y formularios médicos. Cada vez que escaneas uno, puedes estar revelando información sobre dónde estás y qué estás haciendo. La aplicación de escaneo que elijas determina si esa información sigue siendo privada o se monetiza en silencio.

Da el paso. Descarga QR Code Reader Without Ads ahora:

Consigue QR Code Reader Without Ads en Google Play

Consigue QR Code Reader Without Ads en la App Store

Cómo citar: Lubor Šimůnek (2026). *Los riesgos de privacidad de las apps de escaneo QR y cómo evitarlos*. AppStoryo, lapnito.cz s.r.o.. https://appstoryo.com/es/blog/qr-code-scanner-privacy-no-tracking
© 2026 lapnito.cz s.r.o.