QR Kod Tarayıcı Uygulamalarının Gizlilik Riskleri ve Bunlardan Korunma Yolları

Ücretsiz QR tarayıcıların çoğu her taramanızı izler. Hangi verileri topladıklarını ve gerçekten gizli bir tarayıcıyla nasıl korunacağınızı öğrenin.

Yazar: Lubor Šimůnek · Yayınlanma Tarihi: August 9, 2026 · Üretkenlik
Çevrimiçi sürüm: https://appstoryo.com/tr/blog/qr-code-scanner-privacy-no-tracking



QR Tarayıcınız Sizin Hakkınızda Sandığınızdan Fazlasını Biliyor Olabilir

Uygulama mağazasından ücretsiz bir QR kod tarayıcı indirdiğinizde muhtemelen aklınızda tek şey vardır: kolaylık. Gizlilik aklınıza gelen son şeydir. Oysa ilk sırada olmalıdır.

Son birkaç yıl içinde güvenlik araştırmacıları ve gizlilik savunucuları, popüler ücretsiz QR tarayıcı uygulamalarının çoğu kullanıcının hiç fark etmediği agresif veri toplama yöntemleri barındırdığını defalarca ortaya koydu. Bu yazı, bu uygulamaların tam olarak hangi verileri topladığını, bunları nasıl kullandığını ve kendinizi korumak için neler yapabileceğinizi ayrıntılarıyla anlatıyor.

QR Tarayıcı Uygulamaları Gerçekte Hangi Verileri Topluyor?

Yanıt uygulamadan uygulamaya değişir, ancak reklam destekli QR tarayıcıların en sık topladığı veriler şunlardır:

1. Taradığınız QR Kodları

Bu, verilerin en hassas ve aynı zamanda en çok gözden kaçan türüdür. Birçok QR tarayıcı uygulaması taradığınız her kodu kaydeder ve çözümlenmiş içeriği uzak sunuculara gönderir.

Bu içerik; Wi-Fi şifrelerini (QR biçiminde kodlanmış), özel toplantı odası bağlantılarını, doktor randevusu onay kodlarını, kurum içi bağlantıları veya bankacılık ödeme QR kodlarını içerebilir.

Bir doktor muayenehanesinde QR kod taradığınızda ve o bağlantı sessizce bir analiz sunucusuna yüklendiğinde, farkında olmadan sağlığınızla ilgili bir bilgiyi ifşa etmiş olursunuz. Bir ödeme QR kodunu taradığınızda ve bu veri kaydedildiğinde, bu bir finansal ifşadır.

2. Konumunuz

Birçok QR tarayıcı uygulaması hassas GPS konumunuza erişim ister. Görünürdeki gerekçe "kullanıcı deneyimini iyileştirmek"tir, ancak pratikte bu bilgi coğrafi davranış profili oluşturmak için kullanılır: nereye gittiğiniz, o yerlerde ne zaman QR kod taradığınız ve farklı konumlarda ne tür kodlarla karşılaştığınız.

3. Cihaz Tanımlayıcıları

Konum erişimi olmasa bile uygulamalar; cihaz modeli, ekran çözünürlüğü, işletim sistemi sürümü, yüklü uygulama listesi ve reklam kimliğini birleştirerek cihazınızın parmak izini çıkarabilir. Bu parmak izi uygulama yeniden kurulsa bile değişmez ve sizi birden fazla hizmet arasında izlemek için kullanılabilir.

4. Davranışsal Analiz

Popüler QR tarayıcıların çoğu üçüncü taraf analiz SDK'ları içerir; Firebase Analytics, Mixpanel, Amplitude, Adjust veya AppsFlyer yaygındır. Bu SDK'lar uygulamayı ne sıklıkla açtığınızı, hangi özellikleri kullandığınızı, her oturumun ne kadar sürdüğünü ve reklamlarla nasıl etkileşime girdiğinizi kaydeder.

5. Kişilere ve Depolamaya Erişim

Bazı tarayıcı uygulamaları kişilerinize ve depolama alanınıza erişim ister. Kişi listenize erişim, uygulamaların kimliğinizi reklamveren veritabanlarındaki telefon numaraları ve e-posta adresleriyle eşleştirmesine olanak tanır ve profilinizin değerini büyük ölçüde artırır.

İzleme Pikseli Sorunu

Bazı QR tarayıcı uygulamaları daha da ileri giderek taranan bağlantıları gösterdikleri web görünümlerine izleme pikselleri yerleştirir. Bir QR kod taradığınızda ve uygulama hedefi kendi yerleşik tarayıcısında açtığında; çerezleri okuyabilir, JavaScript enjekte edebilir ve hedef web sitesindeki davranışınızı izleyebilir — hem de tamamen sizin haberiniz olmadan.

QR Tarayıcı Gizlilik Sorunlarından Gerçek Örnekler

2020'de yaygın kullanılan bir QR tarayıcı uygulaması, araştırmacıların tarayıcı trafiğini ele geçiren kötü amaçlı yazılım içerdiğini keşfetmesinin ardından Google Play Store'dan kaldırıldı. 2021'de gizlilik araştırmacıları, en çok indirilen birkaç QR tarayıcı uygulamasının taranan bağlantı verilerini veri koruma yasaları zayıf ülkelerdeki sunuculara gönderdiğini tespit etti. 2022'de popüler bir tarayıcı uygulamasının kullanıcının pano içeriğini okuduğu — parolaları ve hassas metinleri ele geçirdiği — ortaya çıktı.

Gizliliğe Saygılı Bir QR Tarayıcı Nasıl Olur?

Gerçekten gizliliğe saygılı bir QR kod tarayıcı şu özelliklere sahiptir:

- **İnternet izni yok** — ağ çağrısı yapamadığı için hiçbir yere veri gönderemez
- **Analiz SDK'sı yok** — ne Firebase, ne Mixpanel, ne AppsFlyer
- **Reklam ağı yok** — ne AdMob, ne Meta Audience Network
- **Asgari izinler** — yalnızca kamera
- **Cihaz üzerinde işleme** — tüm çözümleme yerel olarak yapılır, hiçbir şey aktarılmaz
- **Hesap gerekmez** — tarama geçmişinizin bağlanabileceği bir kimlik yoktur

QR Code Reader Without Ads: Temelden Gizlilik İçin Tasarlandı

QR Code Reader Without Ads tam olarak bu ilkelerle tasarlandı. Uygulamanın internet izni yok — kelimenin tam anlamıyla bir ağ çağrısı yapamıyor — bu da tarama verilerinizi herhangi bir sunucuya göndermesini mimari olarak imkânsız kılıyor. Ne reklam SDK'sı, ne analiz kitaplığı, ne de izleme pikseli var.

QR çözümleme motoru, köklü açık kaynak kitaplıkları kullanarak tamamen cihazınızda çalışır. Bağlantı içeren bir QR kod taradığınızda uygulama, varsayılan tarayıcınızda açmadan önce bağlantıyı incelemeniz için size gösterir.

Hesap gerekmez. Kayıt ekranı yoktur. Tarama geçmişiniz cihazınızda kalır.

Gizli bir QR tarayıcıya geçmeye hazır mısınız? QR Code Reader Without Ads uygulamasını ücretsiz indirin:

Google Play'den indirin — ücretsiz, reklamsız, izlemesiz

iPhone ve iPad için de mevcut:

App Store'dan indirin — ücretsiz, reklamsız, izlemesiz

Mevcut QR Tarayıcınızın Gizliliğini Nasıl Denetlersiniz

Henüz uygulama değiştirmeye hazır değilseniz, mevcut QR tarayıcınızın gizliliğini şöyle değerlendirebilirsiniz:

1. **Uygulama izinlerini kontrol edin** — Ayarlar → Uygulamalar → [tarayıcınız] → İzinler yolunu izleyin. Açık bir işlevsel gerekçe olmadan Konum, Kişiler veya Depolama erişimi varsa bu bir uyarı işaretidir.
2. **Gizlilik politikasını okuyun** — "üçüncü taraf iş ortakları", "reklam ağları" ve "veri paylaşımı" gibi ifadeleri arayın.
3. **Bir ağ izleyici kullanın** — NetGuard (Android) gibi araçlar, uygulamalarınızın hangi alan adlarıyla iletişim kurduğunu gösterir.
4. **Exodus Privacy veri tabanına bakın** — Exodus Privacy, Android APK dosyalarını analiz eder ve her uygulamadaki tüm izleyicileri ve izinleri listeler.

Sonuç Olarak

QR kodlar her yerde: restoran menüleri, etkinlik biletleri, ödeme terminalleri, ürün ambalajları ve sağlık formları. Her tarama yaptığınızda nerede olduğunuza ve ne yaptığınıza dair bilgileri açık etme ihtimaliniz var. Seçtiğiniz tarayıcı uygulaması, bu bilgilerin gizli mi kalacağını yoksa sessizce paraya mı çevrileceğini belirler.

Değişimi yapın. QR Code Reader Without Ads uygulamasını hemen indirin:

QR Code Reader Without Ads uygulamasını Google Play'den edinin

QR Code Reader Without Ads uygulamasını App Store'dan edinin

Kaynak gösterimi: Lubor Šimůnek (2026). *QR Kod Tarayıcı Uygulamalarının Gizlilik Riskleri ve Bunlardan Korunma Yolları*. AppStoryo, lapnito.cz s.r.o..
https://appstoryo.com/tr/blog/qr-code-scanner-privacy-no-tracking
© 2026 lapnito.cz s.r.o.