Zagrożenia dla prywatności ze strony skanerów kodów QR i jak ich uniknąć

Większość darmowych skanerów QR śledzi każde twoje skanowanie. Sprawdź, jakie dane zbierają i jak się chronić dzięki naprawdę prywatnemu skanerowi.

Autor: Lubor Šimůnek · Opublikowano: August 9, 2026 · Produktywność
Wersja online: https://appstoryo.com/pl/blog/qr-code-scanner-privacy-no-tracking



Twój skaner kodów QR może wiedzieć o tobie więcej, niż sądzisz

Kiedy pobierasz darmowy skaner kodów QR ze sklepu z aplikacjami, myślisz zapewne przede wszystkim o wygodzie. Prywatność jest ostatnią rzeczą, która przychodzi ci do głowy. A powinna być pierwszą.

W ciągu ostatnich kilku lat badacze bezpieczeństwa i obrońcy prywatności wielokrotnie wykazywali, że popularne darmowe aplikacje do skanowania kodów QR stosują agresywne praktyki zbierania danych, których większość użytkowników nigdy nie zauważa. Ten artykuł szczegółowo wyjaśnia, jakie dane zbierają te aplikacje, w jaki sposób ich używają i co możesz zrobić, aby się chronić.

Jakie dane naprawdę zbierają aplikacje do skanowania kodów QR?

Odpowiedź zależy od aplikacji, ale najczęściej gromadzone przez skanery QR utrzymywane z reklam dane to:

1. Kody QR, które skanujesz

To najbardziej wrażliwa, a jednocześnie najczęściej pomijana kategoria danych. Wiele aplikacji do skanowania kodów QR zapisuje każdy zeskanowany kod i przesyła odkodowaną treść na zdalne serwery. Treść ta może obejmować hasła Wi-Fi (zakodowane w formacie QR), prywatne adresy URL pokoi spotkań, kody potwierdzające wizyty lekarskie, wewnętrzne linki firmowe czy bankowe kody QR do płatności.

Kiedy skanujesz kod QR w gabinecie lekarskim, a ten adres URL zostaje po cichu wysłany na serwer analityczny, nieświadomie ujawniasz coś o swoim zdrowiu. Kiedy skanujesz płatniczy kod QR, a dane te są rejestrowane, jest to ujawnienie informacji finansowych.

2. Twoja lokalizacja

Wiele aplikacji do skanowania kodów QR prosi o dostęp do dokładnej lokalizacji GPS. Oficjalnie ma to „poprawiać komfort użytkowania", w praktyce jednak służy do budowania profilu geobehawioralnego: dokąd chodzisz, kiedy skanujesz w tych miejscach kody QR i jakie rodzaje kodów napotykasz w różnych lokalizacjach.

3. Identyfikatory urządzenia

Nawet bez dostępu do lokalizacji aplikacje mogą stworzyć odcisk palca twojego urządzenia, łącząc model telefonu, rozdzielczość ekranu, wersję systemu, listę zainstalowanych aplikacji i identyfikator reklamowy. Taki odcisk pozostaje niezmienny nawet po ponownej instalacji aplikacji i pozwala śledzić cię w wielu usługach.

4. Analityka zachowań

Większość popularnych skanerów QR osadza zewnętrzne pakiety SDK do analityki — najczęściej Firebase Analytics, Mixpanel, Amplitude, Adjust lub AppsFlyer. Te pakiety rejestrują, jak często otwierasz aplikację, z jakich funkcji korzystasz, jak długo trwa każda sesja i w jaki sposób reagujesz na reklamy.

5. Dostęp do kontaktów i pamięci

Niektóre skanery proszą o dostęp do kontaktów i pamięci urządzenia. Dostęp do listy kontaktów pozwala aplikacjom powiązać twoją tożsamość z numerami telefonów i adresami e-mail z baz danych reklamodawców, co drastycznie zwiększa wartość twojego profilu.

Problem pikseli śledzących

Niektóre aplikacje do skanowania kodów QR idą jeszcze dalej i osadzają piksele śledzące w widokach internetowych, w których wyświetlają zeskanowane adresy URL. Kiedy skanujesz kod QR, a aplikacja otwiera stronę docelową we wbudowanej przeglądarce, może odczytywać pliki cookie, wstrzykiwać JavaScript i śledzić twoje zachowanie na tej stronie — całkowicie bez twojej wiedzy.

Realne przykłady problemów z prywatnością skanerów QR

W 2020 roku szeroko używana aplikacja do skanowania kodów QR została usunięta ze Sklepu Google Play po tym, jak badacze odkryli, że zawierała złośliwe oprogramowanie

przechwytujące ruch przeglądarki. W 2021 roku badacze prywatności ustalili, że kilka czołowych aplikacji do skanowania kodów QR wysyłało dane zeskanowanych adresów URL na serwery w jurysdykcjach o słabej ochronie danych. W 2022 roku okazało się, że popularna aplikacja skanująca odczytywała zawartość schowka użytkownika, przechwytując hasła i poufne teksty.

Jak wygląda skaner QR szanujący prywatność

Naprawdę prywatny skaner kodów QR ma następujące cechy:

- **Brak uprawnienia do internetu** — nie może wysłać danych nigdzie, ponieważ nie jest w stanie wykonać żadnego połączenia sieciowego
- **Brak pakietów SDK do analityki** — żadnego Firebase, Mixpanela ani AppsFlyera
- **Brak sieci reklamowych** — żadnego AdMob ani Meta Audience Network
- **Minimalne uprawnienia** — wyłącznie aparat
- **Przetwarzanie na urządzeniu** — całe dekodowanie odbywa się lokalnie, nic nie jest przesyłane
- **Brak wymogu konta** — nie istnieje tożsamość, z którą można powiązać historię skanowania

QR Code Reader Without Ads: zbudowany z myślą o prywatności od podstaw

QR Code Reader Without Ads został zaprojektowany dokładnie według tych zasad. Aplikacja nie ma uprawnienia do internetu — dosłownie nie potrafi wykonać połączenia sieciowego — co oznacza, że wysłanie danych z twoich skanów na jakikolwiek serwer jest architektonicznie niemożliwe. Nie ma tu reklamowych pakietów SDK, bibliotek analitycznych ani pikseli śledzących.

Silnik dekodowania kodów QR działa w całości na twoim urządzeniu, korzystając ze sprawdzonych bibliotek open source. Gdy zeskanujesz kod QR zawierający adres URL, aplikacja pokaże ci ten adres do sprawdzenia, zanim otworzy go w twojej domyślnej przeglądarce.

Konto nie jest wymagane. Nie ma ekranu rejestracji. Historia twoich skanów pozostaje na twoim urządzeniu.

Gotowy, by przejść na prywatny skaner QR? Pobierz QR Code Reader Without Ads za darmo:

Pobierz z Google Play — za darmo, bez reklam, bez śledzenia

Dostępny także na iPhone'a i iPada:

Pobierz z App Store — za darmo, bez reklam, bez śledzenia

Jak sprawdzić prywatność swojego obecnego skanera QR

Jeśli nie jesteś jeszcze gotowy na zmianę aplikacji, oto jak ocenić prywatność obecnego skanera QR:

1. **Sprawdź uprawnienia aplikacji** — wejdź w Ustawienia → Aplikacje → [twój skaner] → Uprawnienia. Jeśli ma dostęp do Lokalizacji, Kontaktów lub Pamięci bez wyraźnego uzasadnienia funkcjonalnego, to sygnał ostrzegawczy.
2. **Przeczytaj politykę prywatności** — szukaj sformułowań takich jak „partnerzy zewnętrzni", „sieci reklamowe" i „udostępnianie danych".
3. **Użyj monitora sieci** — narzędzia takie jak NetGuard (Android) pokażą ci, z jakimi domenami komunikują się twoje aplikacje.
4. **Sprawdź bazę Exodus Privacy** — Exodus Privacy analizuje pliki APK Androida i wymienia każdy tracker oraz każde uprawnienie w danej aplikacji.

Podsumowanie

Kody QR są wszędzie — w menu restauracji, na biletach na wydarzenia, w terminalach płatniczych, na opakowaniach produktów i formularzach medycznych. Za każdym razem, gdy skanujesz jeden z nich, potencjalnie ujawniasz informacje o tym, gdzie jesteś i co robisz. To wybrana przez ciebie aplikacja skanująca decyduje, czy te informacje pozostaną prywatne, czy zostaną po cichu spieniężone.

Zmień skaner. Pobierz QR Code Reader Without Ads już teraz:

Pobierz QR Code Reader Without Ads z Google Play

Pobierz QR Code Reader Without Ads z App Store

Jak cytować: Lubor Šimůnek (2026). *Zagrożenia dla prywatności ze strony skanerów kodów QR i jak ich uniknąć*. AppStoryo, lapnito.cz s.r.o.. https://appstoryo.com/pl/blog/qr-code-scanner-privacy-no-tracking
© 2026 lapnito.cz s.r.o.