Jak Sprawdzić, czy Kod QR Jest Bezpieczny, Zanim Go Otworzysz (Przewodnik po Quishingu)

Quishing to phishing przez kod QR. Poznaj sygnały ostrzegawcze przed skanowaniem i co sprawdzić przed naciśnięciem Otwórz.

Autor: Lubor Šimůnek · Opublikowano: August 23, 2026 · Bezpieczeństwo

Wersja online: https://appstoryo.com/pl/blog/qr-code-safe-quishing-guide



Czym jest quishing?

Quishing to phishing realizowany za pomocą kodów QR. Atakujący tworzy kod, który po zeskanowaniu kieruje użytkownika na złośliwą stronę — w celu kradzieży danych logowania, zainstalowania złośliwego oprogramowania lub wyświetlenia fałszywej strony płatności. Nazwa łączy 'QR' i 'phishing', a zagrożenie rośnie, bo ludzie ufają kodom QR niemal bezrefleksyjnie.

Dlaczego kody QR stanowią szczególne ryzyko

W przypadku zwykłego linku możesz najechać kursorem i odczytać URL przed kliknięciem. Z kodem QR nie widzisz celu, dopóki skaner go nie odkoduje — a wiele aplikacji aparatu otwiera przeglądarkę natychmiast, bez wyświetlania adresu. Ta chwila wystarczy złośliwej stronie, by zacząć śledzić Twoje urządzenie.

Kody QR całkowicie omijają też filtry antyspamowe: filtr szuka podejrzanego tekstu lub znanych złośliwych URL-i, ale obraz kodu QR wygląda całkowicie niewinnie. Dlatego e-maile phishingowe coraz częściej zastępują hiperłącza kodami QR, szczególnie w atakach na pracowników firm.

W prawdziwym życiu quishing pojawia się jako naklejki przyklejone nad legalnymi kodami na parkomatach, podrobione menu restauracji, fałszywe awizo przesyłki zostawione w skrzynce pocztowej oraz fałszywe publiczne stacje ładowania zachęcające do 'skanowania w celu płatności'.

Sygnały ostrzegawcze PRZED skanowaniem

- **Naklejka nad oryginalnym kodem.** Naklejka QR przyklejona nad innym kodem to klasyczna podmiana. Delikatnie unieś narożnik — jeśli odstaje, nie skanuj.
- **Język pilności na nieznanej ulotce.** 'Zeskanuj teraz i odbierz nagrodę' lub 'Twoja paczka jest zatrzymana — zeskanuj, by zmienić termin' to taktyki wywierania presji.
- **Niechciana wiadomość e-mail lub list.** Nieoczekiwana komunikacja z banku, firmy kurierskiej lub urzędu, w której kod QR pełni rolę głównego wezwania do działania, to wyraźny sygnał ostrzegawczy.

Co sprawdzić PO zeskanowaniu i PRZED otwarciem

- **Czy domena odpowiada Twoim oczekiwaniom?** Jeśli zeskanowałeś kod QR w banku, URL powinien być na oficjalnej domenie.
- **Czy to skracacz URL?** Serwisy takie jak bit.ly lub tinyurl.com ukrywają prawdziwy cel. Użyj rozszerzarki URL, by poznać rzeczywisty adres przed wizytą.
- **Błędnie napisane lub podrobione domeny.** Zwróć uwagę na paypa1.com (cyfra 1 zamiast litery L) lub g00gle.com (zera zamiast litery O). Czytaj każdy znak uważnie.
- **Podejrzane subdomeny.** login.secure.amazon-dostawa-pl.com wygląda wiarygodnie, ale prawdziwa domena to amazon-dostawa-pl.com, a nie amazon.com.

Jak pomaga QR Code Reader Without Ads

QR Code Reader Without Ads wyświetla pełny podgląd URL przed otwarciem czegokolwiek, dając Ci czas na analizę linku przed podjęciem działania. Jeśli adres wygląda podejrzanie, po prostu nie dotykaj 'Otwórz'. Aplikacja przechowuje lokalną historię skanowań na Twoim urządzeniu, nie zbiera danych i nie wyświetla reklam. Znajdziesz ją w App Store i Google Play, wyszukując 'QR Code Reader Without Ads'.

Pobierz QR Code Reader Without Ads za darmo na iOS lub Android — bez reklam, bez śledzenia i działa całkowicie offline.

Jak cytować: Lubor Šimůnek (2026). *Jak Sprawdzić, czy Kod QR Jest Bezpieczny, Zanim Go Otworzysz (Przewodnik po Quishingu)*. AppStoryo, lapnito.cz s.r.o..
https://appstoryo.com/pl/blog/qr-code-safe-quishing-guide
© 2026 lapnito.cz s.r.o.