Come Capire se un Codice QR È Sicuro Prima di Aprirlo (Guida al Quishing)

Il quishing è il phishing tramite codici QR. Scopri i segnali d'allarme da riconoscere prima di scansionare e cosa verificare prima di toccare Apri.

Autore: Lubor Šimůnek · Pubblicato: August 23, 2026 · Sicurezza
Versione online: https://appstoryo.com/it/blog/qr-code-safe-quishing-guide



Cos'è il quishing?

Il quishing è una forma di phishing che sfrutta i codici QR. Un attaccante crea un codice che, una volta scansionato, rimanda a un sito fraudolento progettato per rubare credenziali, installare malware o simulare una pagina di pagamento. Il termine unisce 'QR' e 'phishing', ed è una delle minacce in più rapida crescita perché le persone si fidano dei QR code quasi istintivamente.

Perché i QR code rappresentano un rischio particolare

Con un link normale puoi passarci sopra il cursore e leggere l'URL prima di cliccare. Con un QR code non vedi la destinazione finché lo scanner non lo decodifica — e molte app della fotocamera aprono subito il browser senza mostrare l'indirizzo. Quel momento basta a un sito malevolo per iniziare a tracciare il tuo dispositivo.

I QR code aggirano anche i filtri antispam: un filtro cerca testo sospetto o URL note come dannose, ma un'immagine di QR code appare del tutto innocua. Ecco perché le e-mail di phishing sostituiscono sempre più spesso i loro link con QR code, soprattutto negli attacchi aziendali.

Nella vita reale il quishing si manifesta in adesivi sopra codici legittimi sui parchimetri, menu

di ristorante contraffatti, avvisi di consegna pacchi lasciati in cassetta postale e false colonnine di ricarica pubbliche che invitano a 'scansionare per pagare'.

Segnali d'allarme PRIMA di scansionare

- **Adesivo sopra un codice originale.** Un QR incollato sopra un altro è uno scambio classico. Sollevate un angolo: se si stacca, non scansionate.
- **Linguaggio d'urgenza su un volantino sconosciuto.** 'Scansiona subito per vincere il tuo premio' o 'Il tuo pacco è fermo — scansiona per riprogrammare' sono tattiche di pressione psicologica.
- **E-mail o lettera non richiesta.** Una comunicazione inaspettata da una banca, un corriere o un ente pubblico con un QR code come principale invito all'azione è un forte segnale d'allarme.

Cosa verificare DOPO aver scansionato e PRIMA di aprire

- **Il dominio corrisponde a ciò che ti aspetti?** Se hai scansionato un QR in una banca, l'URL deve essere sul dominio ufficiale.
- **È un servizio di URL shortening?** Servizi come bit.ly o tinyurl.com nascondono la destinazione reale. Usa un espansore di URL per rivelare l'indirizzo vero prima di visitarlo.
- **Domini con errori ortografici.** Attenzione a paypa1.com o g00gle.com — leggi ogni carattere con attenzione.
- **Sottodomini sospetti.** login.sicuro.amazon-spedizioni-it.com sembra legittimo, ma il dominio reale è amazon-spedizioni-it.com, non amazon.com.

Come aiuta QR Code Reader Without Ads

QR Code Reader Without Ads mostra l'URL completa prima di aprire qualsiasi cosa, dandoti il tempo di analizzare il link. Se l'indirizzo sembra sospetto, non tocchi semplicemente 'Apri'. L'app conserva uno storico locale delle scansioni sul tuo dispositivo, non raccoglie dati e non mostra pubblicità. Disponibile sull'App Store e su Google Play cercando 'QR Code Reader Without Ads'.

Scarica QR Code Reader Without Ads gratis per iOS o Android: senza pubblicità, senza tracciamento e funziona completamente offline.

Come citare: Lubor Šimůnek (2026). *Come Capire se un Codice QR È Sicuro Prima di Aprirlo (Guida al Quishing)*. AppStoryo, lapnito.cz s.r.o.. https://appstoryo.com/it/blog/qr-code-safe-quishing-guide
© 2026 lapnito.cz s.r.o.