MUR
Ministero dell'Università e della Ricerca

CYBER SAPERE

Cyber Security Brochure

QRishing

Le minacce digitali legate alla scansione dei QR Code

Sommario

Cosa troverai in questa brochure

Introduzione

I **QR Code** rappresentano l'evoluzione del tradizionale codice a barre e costituiscono uno strumento efficace per collegare in modo immediato il mondo fisico a quello digitale. Grazie alla loro struttura bidimensionale, possono contenere diverse tipologie di informazioni, quali **link**, **testi**, **contatti** o **contenuti multimediali**, accessibili in pochi secondi tramite smartphone.
La diffusione dei QR Code è aumentata rapidamente grazie all'uso sempre più frequente dei dispositivi mobili, rendendo la loro scansione un gesto semplice, veloce e ormai parte delle abitudini quotidiane.

I **QR Code** possono essere **statici o dinamici**. Particolarmente rilevanti sono quelli dinamici, che hanno trasformato strumenti tradizionalmente statici, come brochure, menù e volantini, in contenuti digitali aggiornabili nel tempo senza necessità di ristampa. I QR Code dinamici inoltre consentono di raccogliere dati sulle scansioni, utili per migliorare l'efficacia comunicativa. Tuttavia, è fondamentale prestare attenzione alla sicurezza, poiché un QR Code apparentemente innocuo può nascondere rischi informatici, richiedendo un utilizzo consapevole da parte degli utenti.

Lo sapevi?

Nel 2025 il 12% di tutti gli attacchi di phishing conteneva un QR Code

Le modalità di attacco tramite QR Code:

Creazione di un QR Code falso
L'attaccante genera un codice QR che reindirizza verso un sito malevolo appositamente creato, indistinguibile da uno legittimo.

Distribuzione del QR
Il codice viene diffuso tramite e-mail di phishing, poster fisici contraffatti o messaggi ingannevoli.

Scansione da parte della vittima
Scansione da parte dell'utente del codice senza verificare la fonte e il link a cui rimanda.

Reindirizzamento a una pagina fraudolenta
La vittima viene indirizzata su pagine web che imitano portali legittimi con l'obiettivo di sottrarre credenziali o dati sensibili.

Fonte: 2026 QR Code Phishing Trends - di KeepNet Labs

Quali sono i rischi?

Rischi

01 Perdita di credenziali e dati sensibili

Scansionando un **QR Code malevolo**, potresti essere reindirizzato a **siti web contraffatti**, spesso progettati per imitare portali ufficiali. Su tali siti può essere richiesto l'**inserimento di credenziali di accesso o altre informazioni sensibili**, che vengono **raccolte dai criminali informatici** e successivamente sfruttate per compiere attività fraudolente.

02 Installazione di malware

Tramite la scansione di QR Code fraudolenti è possibile che vengano scaricati sul tuo dispositivo software dannosi (es. spyware) che sono in grado di compromettere la sicurezza del sistema. In questo modo i criminali informatici possono avere accesso ai file presenti sul dispositivo, alla fotocamera, al microfono o tracciare le tue attività.

03 Frodi finanziarie

Alcuni attacchi QRishing reindirizzano verso **pagine di pagamento false** o sostituiscono QR Code legittimi (es. su bollettini, POS, parcheggi) con **codici fraudolenti**, **dirottando transazioni** reali verso conti controllati dall'attaccante.

Contromisure

Verifica la provenienza e l'integrità del QR Code prima della scansione, controlla che non sia stato **sovrapposto**, **sostituito** o **alterato** e che provenga da una fonte affidabile

Inquadra il QR Code prestando attenzione all'anteprima del **link di reindirizzamento**: potrai verificare l'attendibilità dell'**URL** ed evitare di accedere a siti ricreati ad hoc dai criminali informatici

Diffida dalle **richieste di pagamento** che propongono come unico metodo la **scansione di un QR Code**: eviterai di cadere vittima di truffe finalizzate al furto di dati bancari

03

Come difendersi?

Usa applicazioni sicure

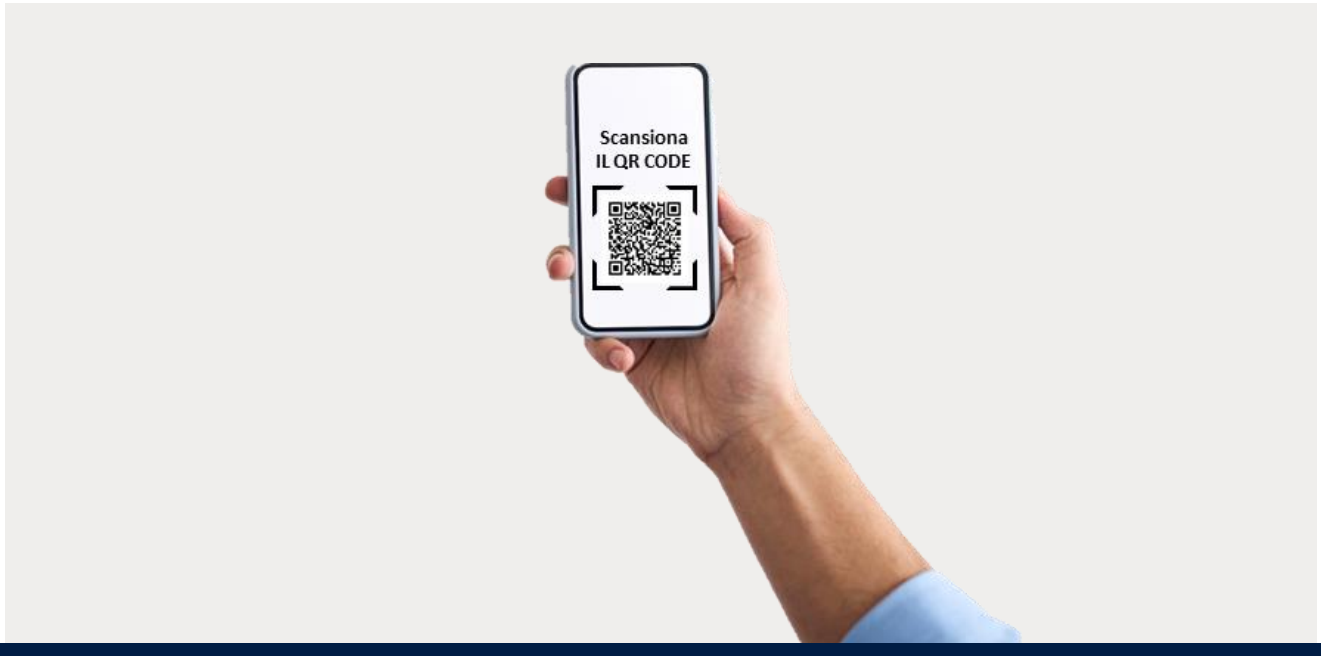
Quando decidi di **scansionare un QR Code**, utilizza un'**applicazione affidabile e sempre aggiornata** in grado di analizzare il collegamento prima di aprirlo, così da **individuare** eventuali **siti web malevoli o malware nascosti**. Questa semplice precauzione ti consente di navigare in modo più sicuro e di ridurre il rischio di cadere vittima di truffe informatiche.

Verifica la fonte

Non inserire **informazioni personali** o **dati sensibili**, senza aver prima verificato la **legittimità** del **sito** o della **fonte**. Prendersi qualche secondo in più per controllare è un modo semplice ed efficace per **proteggere te stesso e i tuoi dati.**

Presta attenzione

Fai attenzione ai **QR Code** che trovi negli **spazi pubblici**, su post, volantini, o che ricevi tramite messaggi non verificati. Questi possono sembrare innocui, ma nascondono spesso **link pericolosi**. È sempre consigliato verificare il QR Code prima di scansionarlo.



Security Trend

QR Code sui parchimetri di Pesaro

Nel maggio 2026 è stato individuato a Pesaro un caso di QRishing.
L'attacco ha coinvolto alcuni **parchimetri della città, sui quali erano stati applicati adesivi con codici QR fraudolenti**, sovrapposti a quelli originali destinati al pagamento della sosta.
Gli utenti, convinti di utilizzare il servizio ufficiale, scansionavano il QR Code per pagare il parcheggio.
In realtà venivano reindirizzati a un **sito web falso**, progettato per imitare il portale legittimo del servizio di pagamento.
All'interno della pagina venivano **richiesti dati personali** e della **carta di credito**.
In questo modo gli attaccanti potevano raccogliere le informazioni inserite dagli utenti e utilizzarle per effettuare attività fraudolente o sottrarre denaro.
La truffa è stata rilevata dal gestore del servizio di parcheggio, che ha provveduto alla rimozione immediata dei QR Code contraffatti e alla segnalazione dell'incidente alle autorità competenti.

Maggio 2026

QR Code fraudolenti in lettere bancarie

Nel 2025 in Germania sono stati segnalati diversi casi di QRishing.
In particolare, i criminali hanno diffuso **lettere cartacee false apparentemente inviate da banche**.
In questi documenti veniva richiesto ai clienti di aggiornare o verificare le proprie **credenziali di home banking tramite un QR Code** inserito nella comunicazione.
Scansionando il codice, le vittime venivano indirizzate a un **sito web contraffatto**, molto simile a quello ufficiale dell'istituto bancario.
Una volta inseriti username e password, i dati venivano acquisiti dagli attaccanti, che potevano accedere ai conti correnti e compiere operazioni fraudolente.
Inoltre, il QR Code nascondeva l'indirizzo del sito fino al momento della scansione, rendendo più difficile riconoscere la frode.
Questo tipo di attacco si è dimostrato particolarmente efficace perché sfruttava la fiducia degli utenti verso la posta fisica, che viene spesso percepita come più sicura rispetto alle comunicazioni digitali.

2025

MUR
Ministero dell'Università e della Ricerca

CYBER SAPERE

Restate sintonizzati:

nuovi approfondimenti sulla cybersecurity vi aspettano nelle prossime pubblicazioni.