MUR

CYBER
SAPERE

Cyber Security Brochure

QRishing

Digital threats linked to scanning QR Codes

Summary

What you will find in this brochure

Introduction

QR Codes represent the evolution of the traditional barcode and are an effective tool for immediately connecting the physical world with the digital one. Thanks to their two-dimensional structure, they can contain different types of information, such as links, text, contacts or multimedia content, accessible in a few seconds via smartphone.

The spread of QR Codes has grown rapidly thanks to the increasingly frequent use of mobile devices, making scanning a simple, quick gesture that is now part of everyday habits. QR Codes can be static or dynamic. Dynamic QR Codes are particularly relevant because they have transformed traditionally static tools, such as brochures, menus and flyers, into digital content that can be updated over time without reprinting. However, it is essential to pay attention to security because an apparently harmless QR Code may hide cyber risks and requires conscious use by users.

Attack methods through QR Codes

1. **Creation of a fake QR Code:** The attacker generates a QR Code that redirects to a malicious site designed to be indistinguishable from a legitimate one.
2. **QR distribution:** The code is spread through phishing emails, counterfeit physical posters or deceptive messages.
3. **Victim scanning:** The user scans the code without verifying the source and the link it redirects to.
4. **Redirect to a fraudulent page:** The victim is sent to web pages that imitate legitimate portals to steal credentials or sensitive data.

Did you know?

12%

In 2025, 12% of all phishing attacks contained a QR Code.

Source: 2026 QR Code Phishing Trends - KeepNet Labs

What are the risks?

Risks

01 Loss of credentials and sensitive data

By scanning a malicious QR Code, you may be redirected to counterfeit websites that often imitate official portals. Such sites may ask you to enter access credentials or other sensitive information, which is collected by cybercriminals and then exploited for fraudulent activities.

02 Malware installation

By scanning fraudulent QR Codes, malicious software such as spyware may be downloaded to your device and compromise system security. In this way, cybercriminals may access files on the device, the camera, the microphone or track your activities.

03 Financial fraud

Some QRishing attacks redirect to fake payment pages or replace legitimate QR Codes, for example on bills, POS terminals or parking meters, with fraudulent codes that divert real transactions to accounts controlled by the attacker.

Countermeasures

Verify the source and integrity of the QR Code before scanning it. Check that it has not been overlaid, replaced or altered and that it comes from a trusted source.

Frame the QR Code while paying attention to the preview of the redirect link, so you can check the reliability of the URL and avoid sites created by criminals.

Be wary of payment requests that offer QR Code scanning as the only method. This helps you avoid scams designed to steal banking data.

How to protect yourself?

Use secure applications

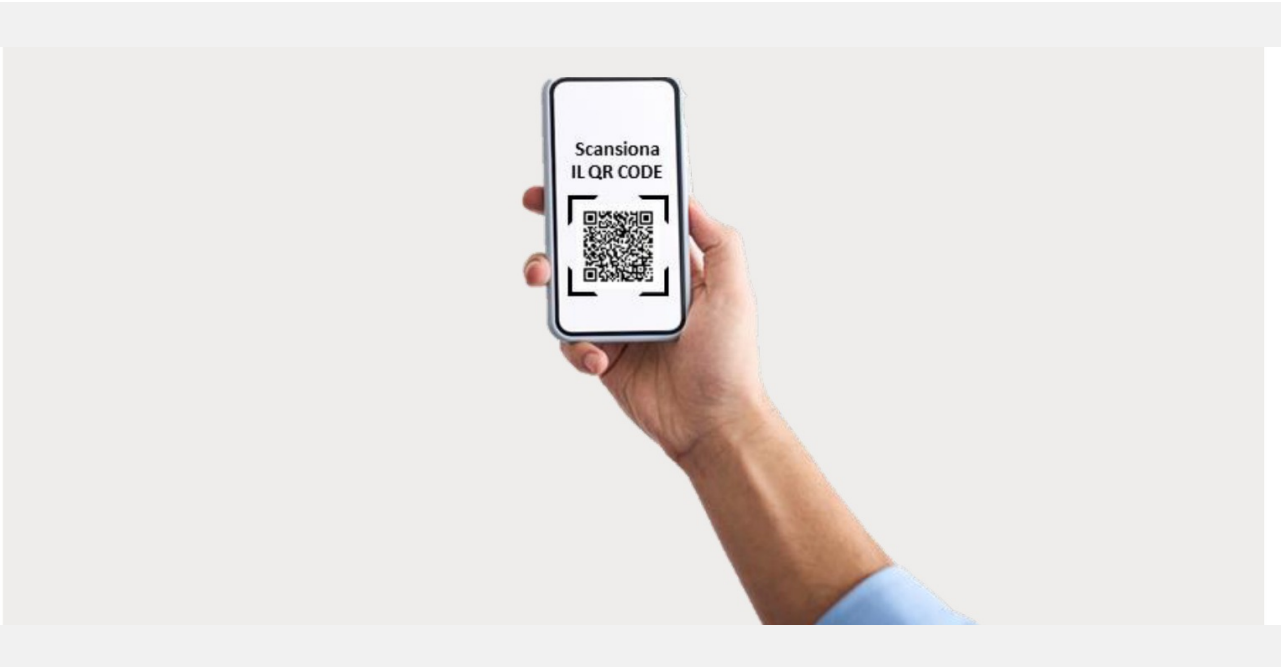
When scanning a QR Code, use a reliable and always updated application that can analyze the link before opening it, helping identify malicious websites or hidden malware. This simple precaution allows safer browsing and reduces the risk of cyber scams.

Verify the source

Do not enter personal information or sensitive data without first verifying the legitimacy of the site or source. Taking a few extra seconds to check is a simple and effective way to protect yourself and your data.

Pay attention

Be careful with QR Codes found in public spaces, on posts or flyers, or received through unverified messages. They may look harmless but often hide dangerous links. Always verify the QR Code before scanning it.



Security Trend

QR Codes on parking meters in Pesaro

In May 2026, a QRishing case was identified in Pesaro. The attack involved some parking meters in the city, where stickers with fraudulent QR Codes had been placed over the original ones used for parking payment. Users, convinced they were using the official service, scanned the QR Code to pay for parking. Instead, they were redirected to a fake website designed to imitate the legitimate payment portal. The page requested personal data and credit card information. In this way attackers could collect the information entered by users and use it to perform fraudulent activities or steal money. The scam was detected by the parking service operator, which removed the counterfeit QR Codes and reported the incident to the competent authorities.

Fraudulent QR Codes in bank letters

In 2025, several QRishing cases were reported in Germany. Criminals distributed fake paper letters that appeared to come from banks. These documents asked customers to update or verify their home banking credentials through a QR Code included in the communication. By scanning the code, victims were redirected to a counterfeit website very similar to the official banking site. Once username and password were entered, the data was captured by attackers, who could access current accounts and carry out fraudulent transactions. The QR Code also hid the site address until scanning, making the fraud harder to recognize. This attack was particularly effective because it exploited users' trust in physical mail, often perceived as safer than digital communications.

May 2026

2025

MUR
Ministero dell'Università e della Ricerca

CYBER SAPERE

Stay tuned:
new cybersecurity insights
await you
in upcoming publications.