

QR Code Phishing Attacks



Photo by [Proxyclick Visitor Management System](#) on [Unsplash](#)

A QR code phishing attack is a type of scam that uses QR codes to trick people into visiting malicious websites or giving away their personal information. QR codes are square-shaped images that can be scanned by a smartphone camera to access a website, app, or other service.

However, some hackers create fake QR codes that look like they offer something useful or interesting, but actually lead to phishing sites that try to steal your login credentials, credit card details, or other sensitive data.

Below is some examples for QR code:



Payload: **<https://www.thehackingblog.net>**

It is my personal blog about cybersecurity and ethical hacking. This URL should be safe.



Payload: **<https://www.nashruddinamin.com>**

It is my personal website and the URL should be safe.



Payload: **<https://testsafebrowsing.appspot.com/s/malware.html>**

The URL should be unsafe, opening the URL should trigger Google Safe Browsing and display warnings about malware.



Payload: **<https://testsafebrowsing.appspot.com/s/phishing.html>**

The URL should be unsafe, opening the URL should trigger Google Safe Browsing and display warnings about the site being a phishing website.