Quishing – How to Avoid QR Code Scams

What is a QR code?

A QR code (short for *Quick Response code*) is a type of barcode made up of black and white squares that can be scanned using a smartphone camera.

When scanned, a QR code usually opens a website, but it can also trigger a payment page, download an app, or open a message.

QR codes are widely used for things like restaurant menus, parking payments, event registration, Wi-Fi access and marketing information.

The QR code on the right is the author's LinkedIn profile. Open your phone's camera, focus it on the QR code and a yellow bar with LinkedIn written in it will appear. Click this and you'll be taken to my profile on the LinkedIn website.

QR codes themselves are not dangerous. The risk comes from where the code takes you once it is scanned.

What is quishing?

Quishing is a form of scam that uses QR codes instead of clickable links. Criminals create or replace QR codes so that, when scanned, they send you to a fake website designed to steal personal information, passwords, or bank and card details, or to install malicious software on your phone.

It's most found on parking meters, charging points, restaurant tables, posters, letters and emails. Fake QR codes are often placed over genuine ones or sent in messages that appear to come from trusted organisations such as banks, delivery firms or government bodies.

How to protect yourself from quishing

You can significantly reduce your risk by adopting a few simple habits.

- **Be healthily sceptical** - Do not assume a QR code is safe just because it appears in a public place or looks professional. A QR code on a parking meter, hotel room table or email can still be fake.
- **Check physical QR codes carefully** - Before scanning, look closely at the code. Be cautious if it appears to be a sticker, looks misaligned, has rough edges, or seems to be placed over another code. These are common signs of tampering.
- **Be especially cautious with QR codes in emails or messages** - Banks, online services and government bodies rarely ask you to scan a QR code to secure an account or make an urgent payment. Messages that create pressure or panic are a strong warning sign.

- **Always check the web address** - Most phones show a preview of the website address before opening it. If the address looks strange, misspelt, shortened, or does not match the organisation it claims to be from, do not continue.
- **Avoid entering passwords or payment details** - If a QR code takes you to a page asking for login details, card numbers or personal information, stop. Instead, visit the organisation's website directly by typing the address yourself or using their official app.
- **Use trusted alternatives** - For parking or payments, use well-known official apps downloaded from the Apple App Store or Google Play, rather than scanning QR codes on signs or machines.

What to do if you think you've scanned a fake QR code

Stop immediately. Do not enter any information. If you have already entered details, change your passwords on the genuine website as soon as possible and contact your bank if financial information may have been compromised. Suspicious QR codes and scams can be reported via the Report Fraud website (which has lots of sources of help) or your local police service.

This was researched by AI using consumer protection and UK police guidance then written for Charity Excellence where it was checked and edited by a human