



QR Code Scams

QR codes, like the one at the bottom of this page, are a popular way of allowing customers and visitors to access information or services without having to type a long sequence of letters and punctuation. QR Code scams are sometime referred to as Quishing attacks.

QR Codes are used for a variety of links including: recipes page from a packet; access to Wi-Fi; download a restaurant menu; open a location map; download apps; display adverts; access bus/train timetables; share business card; invite feedback; scan to pay and more.

The last-mentioned (scan to pay) is an area where scammers have tried to mislead consumers by, for example, fixing their own QR Code on top of a legitimate one so the the person wishing to pay (for parking for example) will be directed to a malicious web site and lose any money to the scammers.

Protecting yourself from QR Code Scams:

Examine external signs carefully to see if the original QR Code may have been pasted over

Before clicking the link in your camera app, review the target domain name looking, particularly, for spelling errors and a divergence from that which you expected

If paying using a QR Code check the amount and beneficiary before clicking 'Pay'

For more official advice on QR Code Scams, scan the QR Code below (or click [here](#)):



More on QR Code scams