

Scams & online safety | Easy | 2 min read

Fake QR code scams

QR codes are those square black and white patterns you scan with your phone camera. Most are perfectly safe, but criminals sometimes use them to send people to fake websites.

Where the risk is

- Stickers placed over the real QR code on a car park payment machine.
- Codes in unexpected emails, letters or text messages.
- Codes on posters or flyers in public places that promise prizes or discounts.
- Codes sent by a "bank" or "delivery company".

Why it works

You cannot read a QR code with your eyes, so you cannot tell where it leads until you scan it. A fake one can take you to a page that looks like a real payment page and collects your card details.

Staying safe

1. **Look at the web address that appears** after you scan, before you tap it. Does it match the company? Is it spelt correctly?
2. Check whether a sticker has been placed over the original code. If it looks peeled, bumpy or added on, do not use it.
3. In a car park, you can often pay with the official app downloaded from your phone's app store, or by phone or cash instead.
4. Do not scan codes from messages you were not expecting.
5. Never enter card details, passwords or codes after a QR scan unless you are sure of the website.

Tip for restaurants and events

A code on a restaurant table is usually fine. If it asks for a lot of personal details, just ask staff for a paper menu.

If you scanned a bad code

Close the page and do not type anything in. If you entered card details, ring your bank on 159 or the number on your card. If you entered a password, change it on the real website. You can report scams to Report Fraud (formerly Action Fraud) at reportfraud.police.uk or on 0300 123 2040, or Police Scotland on 101.

When to get more help

If you are not sure about a code, or you would like us to show you how to check a link on your phone, just ask.

Still stuck? Email admin@visiontech336.com and tell us what you can see on the screen. Menus and button names can differ slightly between versions and makes. If something does not match, stop and ask rather than guess. Please never send passwords or card details.