New quishing alert: £3.5 million lost last year to fraudulent QR codes

Action Fraud is urging people to look out for rogue QR codes, after 784 reports of 'quishing' were made to Action Fraud between April 2024 and April 2025, with almost £3.5 million lost.



A new alert has been issued by Action Fraud, warning about quishing, a form of phishing where a fraudulent QR code is scanned, designed to steal personal and financial information. The warning encourages people to stay vigilant and double check QR codes to see if they are malicious, or have been tampered with, before scanning them online or in public spaces.

Claire Webb, Acting Director of Action Fraud, said:

"QR codes are becoming increasingly common in everyday life, whether it's scanning one to pay for parking, or receiving an email asking to verify an online account. However, reporting shows cyber criminals are increasingly using quishing as a way to trick the public out of their personal and financial information.

"We're urging people to stop and check before scanning QR codes, to avoid becoming a victim of quishing. Look out for QR codes that may have been tampered with in open spaces, or emails and texts that might include rogue codes. If you're in doubt, contact the organisation directly. You can follow our advice on quishing, on our website at www.actionfraud.police.uk to help protect yourself."

Action Fraud can reveal that quishing happens most frequently in car parks, with criminals using stickers to tamper with QR codes on parking machines. Quishing also occurred on online shopping platforms, where sellers received a QR code via email to either verify accounts or to receive payment for sold items.

Reports also showed phishing attacks were taking place impersonating HMRC, or other UK government schemes, targeting people with QR codes designed to steal personal and financial details.

What can you do avoid being a victim of quishing?

- QR codes used in pubs or restaurants are usually safe to scan.

- Scanning QR codes in open spaces (like stations and car parks) might pose a greater risk. Check for signs that codes may have been tampered with (usually by a sticker placed over the legitimate QR code). If in doubt, do not scan them: use a search engine to find the official website or app for the organisation you need to make a payment to.

- If you receive an email with a QR code in it, and you're asked to scan it, you should be cautious due to an increase in these types of 'quishing' attacks.

- Finally, we recommend that you use the QR-scanner that comes with your phone, rather than using an app downloaded from an app store.

If you receive a suspicious email, report it by forwarding it to phishing@report.gov.uk

Find out how to protect yourself from fraud: https://stopthinkfraud.campaign.gov.uk

If you've been a victim of fraud, report it at www.actionfraud.police.uk or by calling 0300 123 2040. In Scotland, contact Police Scotland on 101.

Message Sent By
Action Fraud