New quishing alert: £3.5 million lost last year to fraudulent QR codes [#459071134]

alert@neighbourhoodalert.co.uk | FRI JUN 20 2:46 PM | 5 minute(s) read

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

Action Fraud is urging people to look out for rogue QR codes, after 784 reports 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
QR code is scanned, designed to steal personal and financial information. The w
stay vigilant and double check QR codes to see if they are malicious, or have be
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 sca
parking, or receiving an email asking to verify an online account. However, repo
are increasingly using quishing as a way to trick the public out of their personal

“We’re urging people to stop and check before scanning QR codes, to avoid bec
Look out for QR codes that may have been tampered with in open spaces, or em
include rogue codes. If you’re in doubt, contact the organisation directly. You ca
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, witl tamper with QR codes on parking machines. Quishing also occurred on online s sellers received a QR code via email to either verify accounts or to receive payn

Reports also showed phishing attacks were taking place impersonating HMRC, schemes, targeting people with QR codes designed to steal personal and financi

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

that codes may have been tampered with (usually by a sticker placed over the le doubt, do not scan them: use a search engine to find the official website or app f to make a payment to.

- If you receive an email with a QR code in it, and you're asked to scan it, you

increase in these types of 'quishing' attacks.

- Finally, we recommend that you use the QR-scanner that comes with your pl

app downloaded from an app store.

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

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

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

Message Sent By
Action Fraud

Reply

Useful or not?

Share

To login to your account click here, to report a fault click here, or unsubscribe

You are receiving this message because you are registered on Wiltshire and Swindon Community Messaging. Various organisations are licensed to send messages via this system, we call these organisations "Information Providers". Please note that this message was sent by Action Fraud (NFIB) and that Action Fraud (NFIB) does not necessarily represent the views of Wiltshire and Swindon Community Messaging or other Information Providers who may send you messages via this system.

You can instantly review the messages you receive and configure which Information Providers can see your information by clicking here, or you can unsubscribe completely, (you can also review our terms and conditions and Privacy Policy from these links).

This email communication makes use of a "Clear Image"(gif) to track results of the email campaign. If you wish to turn off this tracking for future emails, you can do so by not downloading the images in the e-mail itself. All links in the body of this email are shortened to allow click through monitoring.

VISAV Limited is the company which built and owns the

Neighbourhood Alert platform that powers this system. VISAV's authorised staff can see your data and is registered with the Information Commissioner's Office as the national Data Controller for the entire database. VISAV needs to see your data in order to be able to manage the system and provide support; it cannot use it for commercial or promotional purposes unless you specifically opt-in to Membership benefits. Review the website terms.