THAMES VALLEY POLICE

TV Alert

"Quishing for Trouble: When Scanning Leads to Scams" - Police warn of QR code fraud

Thames Valley Police are urging the public to remain vigilant to fraudulent QR codes which can easily turn from convenience to con.

'Quishing' or 'QR Code Phishing', involves tricking someone into scanning a QR code which once scanned, will take you to a bogus website where you innocently input your details thinking you are paying for a service or visiting the genuine site, when in fact, you are unknowingly sharing all your personal details with criminals, which could lead to Identity fraud

QR codes are often found on things like parking machines, charging points, emails, even restaurant menus.

Detective Inspector Duncan Wynn, Head of Central Fraud Unit at Thames Valley Police said:

"While QR codes offer a convenient option for saving time, they can lead to fraud if they have been tampered with by fraudsters.

I encourage you to take a moment to stop! think fraud when reaching to scan a code.

- If the QR code is on a poster in a public area, always check whether it appears to have been stuck over the original. If the sign or notice is laminated and the QR code is under the lamination or part of the original print, chances are it is more likely to be genuine.

- If in doubt, download the app from the official Google or Apple store or search the website on your phone's internet browser, rather than scanning a QR code to take you there. It may take longer, but it is more secure.

- Check the preview of the QR code's URL to see if it appears legitimate. Make sure the website uses HTTPS rather than HTTP, does not have obvious misspellings and has a trusted domain.
- Use your phone's built-in QR scanner (available in most Camera apps) rather than downloading third-party QR scanning apps, which can sometimes be risky.
- Trust your instincts. If something does not seem right, do not scan, alert the owner of the QR code and police by calling 101 to report. "

Quishing can also occur on online shopping platforms, where sellers received a QR code via email to either verify accounts or to receive payment for sold items.

Fraudsters may impersonate banks, or other UK government organisations such as HMRC. If you receive an email with a QR code in it, and you are asked to scan it, you should be cautious due to an increase in these types of 'quishing' attacks.

Detective Inspector Duncan Wynn, continues:

"Resolving identity fraud, which can happen because of scanning a fraudulent QR code is often a lengthy and complex process.

When criminals use stolen personal details to obtain financial products such as loans or credit cards, victims can face significant challenges in proving their identity, restoring their credit profile, and regaining financial security.

This can take considerable time and effort, underscoring the importance of vigilance and preventative measures."

Taking an extra few moments to double-check really can save time overall."

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 have 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.