CYBER ALERT: Beware "Quishing" Scams Using QR Codes

Devon & Cornwall Police is warning residents about a growing cyber threat known as **"Quishing"**, where criminals use QR codes to direct people to fraudulent websites designed to steal personal, financial or account login information.

A QR code may appear safe because it avoids the suspicious links traditionally seen in phishing emails. However, scanning a malicious QR code can take you to a fake website that looks genuine and may ask you to enter passwords, payment card details, or other personal information.

How Quishing Scams Work

Criminals may send QR codes via:

- Email messages claiming to be from trusted organisations.
- Fake parcel delivery notifications.
- Banking security alerts.
- Utility company invoices.
- Account verification requests.
- Printed letters, posters, or stickers placed over legitimate QR codes.

Warning Signs

Be suspicious if a QR code:

- Arrives unexpectedly.
- Claims urgent action is required.
- Promises a refund, reward, or prize.
- States that an account will be suspended unless you act immediately.

- Requests account credentials or payment details after scanning.

How to Protect Yourself

Think before you scan.

Verify who sent the message.

Preview the website address if your phone offers this option.

Check that the web address matches the genuine organisation.

Never enter passwords, banking details, or one-time passcodes unless you are absolutely certain the website is legitimate.

If in doubt, visit the organisation's website directly using your browser rather than scanning the QR code.

If You Have Scanned a Suspicious QR Code

If you entered login or payment details after scanning a QR code:

- Change your passwords immediately.
- If financial details were provided contact your bank by calling **159**
- Enable Two-Step Verification (2SV) / Multi-Factor Authentication (MFA) on affected accounts.
- Regularly monitor all your accounts for unusual activity.
- Report the incident to Report Fraud.

Reporting

Forward suspicious emails to: **report@phishing.gov.uk** and suspicious texts to **7726**.

Report fraud or cybercrime to Report Fraud: **UK's Home for Reporting Cyber Crime & Fraud - Report Fraud** 0300 123 2040

Remember

QR codes are simply another way of delivering a web link. Treat every unexpected QR code with the same caution you would apply to an unexpected email link.

STOP • THINK • VERIFY Taking a few moments to independently verify, then double check, before scanning can prevent your personal information or money from falling into the hands of criminals. IF IN ANY DOUBT DON'T SCAN.

Reply Share Rate



Message Sent By
Mick Harrison
(Devon & Cornwall Police, Cyber Protect Officer, Devon & Cornwall)