POLICE - ALERT

QR (Quick Response) Codes as enablers of fraud

QR codes or 'Quick Response' codes work when the user scans them via a digital device, usually a smartphone. They are widely used for quickly directing users to websites, logging into devices, or ordering or paying for goods and services.

Cyber criminals are increasingly using QR technology to scam victims, by creating their own malicious QR codes designed to trick people into handing over banking or personal information.

Analysis of Action Fraud reports reveals that the majority of QR code related fraud tends to happen in open spaces, such as car parks or parking meters. A common scam involves malicious QR code stickers being placed on top of a legitimate one at car parks. The QR codes link to genuine-looking payment sites that steal personal and financial information. We are also seeing an increase in the number of phishing emails using QR codes.

Between October 2023 to June 2024, Action Fraud received 199 reports relating to a fraudulent activity involving a QR code.

CLASSIFICATION - SUITABLE FOR PUBLICATION

Advice on how to use QR codes safely

•The QR codes used in pubs or restaurants are probably safe for you to scan.

• Scanning QR codes in open spaces (like stations and car parks) might be riskier. Check for tampered QR codes (stickers), 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 exercise caution as we are seeing an increase in these types of 'quishing' attacks.

• When scanning a QR code, use the QR-scanner that comes with your phone, rather than using an app downloaded from an app store.

For further information on using QR codes safely see:
'How to use QR codes safely' guidance from the Canadian Centre for Cyber Security.