ISSUE 64

SCAMS AWARENESS NEWSLETTER

MARCH 2026

WELCOME TO OUR

Monthly Newsletter

In this newsletter:

- Why QR codes can be risky and common scams p.2
- How to protect yourself p.3
- New tools, what to do and a three-step rule p.4

QR Code Scams: Convenient technology – or a hidden risk?

QR codes are everywhere. On parking machines. On restaurant tables. On parcels. In emails. Even on posters at bus stops. They were originally designed to make life easier - simply point your phone camera at the square black-and-white code and you are taken directly to a website. But criminals have learned how to exploit that convenience.

In recent months, police and fraud prevention bodies across the UK have reported a sharp increase in QR code fraud - sometimes called "quishing" (QR phishing). While anyone can be targeted, fraudsters often rely on the fact that many people are still becoming familiar with how QR codes work.

This month's newsletter explains how QR fraud works, the common scenarios to watch for, and - most importantly - how to protect yourself.

Cheshire Age UK Let's change how we age

Cheshire West and Chester

Report Fraud

Cheshire East Council Trading Standards

Why QR codes can be risky

When you click on a website link in an email, you can usually see the web address (for example, www.ageuk.org/cheshire). Even if you don’t study it closely, it is visible.

With a QR code, you cannot see where it will take you until after you scan it. That’s the weakness criminal’s exploit.

A QR code is simply a shortcut to a website. It does not tell you whether that website is genuine, fake, or malicious. Your phone will open whatever address is embedded inside it - good or bad.

Fraudsters use this to:

- Direct you to fake payment pages
- Capture your banking details
- Install malicious software
- Steal login credentials

And because scanning feels quick and modern, people often do it without pausing to think.

Common QR scams

1. Fake parking meter QR Codes

Criminals place a sticker containing their own QR code over the genuine code on a parking machine. When you scan it, you are taken to a fake website that looks like a legitimate parking payment service.

You enter your card details, thinking you are paying for parking - but the money and your card information go straight to the fraudsters.

In some cases, victims only realise days later when suspicious transactions appear on their bank statement, or they receive a parking penalty notice.

2. QR Codes in emails claiming to be from trusted organisations

Fraudsters increasingly send QR codes instead of links, claiming to be from HMRC, Royal Mail, NHS, or banks. The email may warn of taxes, missed deliveries, or appointments. Instead of a link, it instructs you to “scan the QR code below.”

This tactic is deliberate. Many email security systems are better at detecting suspicious links than suspicious QR images.

Once scanned, you are taken to a convincing fake website asking for personal or financial details.

How to protect yourself from QR fraud

1. Pause before you scan

If you did not request the QR code, or if it appears unexpectedly, stop and think.

Ask yourself:

- Why am I being asked to scan this?
- Could I reach this organisation another way?

If the message creates urgency (“Pay immediately”, “Last chance”, “Account suspended”), that is a red flag.

2. Inspect physical QR codes carefully

If you are using a QR code on a parking machine or public surface:

- Check for stickers placed on top of other stickers
- Look for signs of tampering
- Compare with nearby machines

If something looks poorly applied or misaligned, do not scan it. Instead, use an official parking app you have already downloaded, or pay via card machine if available.

3. Never enter banking passwords after scanning a QR code

Legitimate organisations do not require you to enter full banking passwords via a random QR code scan.

If a page asks for:

- Full online banking passwords
- One-time passcodes sent to your phone
- Card PIN numbers

Stop immediately.

No legitimate organisation will ask for these in that way.

4. Go Directly to the official website

Instead of scanning a QR code in an email or text, manually type the organisation’s official website address into your browser.

For example:

- For tax matters, go directly to GOV.UK
- For deliveries, visit the courier’s official website
- For healthcare matters, log in through official NHS channels

Do not rely on links or codes provided in unexpected messages.

5. Check the web address after scanning

If you do scan a QR code, look carefully at the website address before entering any details.

Fraudulent websites often:

- Use slight spelling changes
- Include extra words or numbers
- Use unusual endings instead of .co.uk

If the address looks strange, close the page immediately.

6. Be cautious about QR codes asking for payment

QR codes are common for menus, app downloads, or Wi-Fi, but rarely for financial payments.

If you are being asked to pay a fine, tax bill, delivery fee or parking charge via a QR code in an email or text, treat it as suspicious.

Treat requests for fines, taxes, delivery fees, or parking charges with caution.

New tools to help protect against QR fraud

While awareness and caution are the best first lines of defence, there are also tools designed to help protect us from the rise in QR fraud. One such resource is QR Siren, founded by experts in artificial intelligence and cyber security. Their mobile app services are free to use and provide helpful guidance for checking QR codes before scanning. We share this as a resource to support your safety and are not affiliated with or funded by QR Siren.

What to do if you've scanned is a suspicious QR code

If you have entered financial information:

- Contact your bank immediately — use a number you know is correct or call 159.
- Explain that you may have been a victim of fraud.
- Monitor your accounts for any unusual transactions.
- Where possible, report the incident to the company or organisation involved (for example, a restaurant, council, or delivery company).

If you have shared personal information, consider reporting it to Report Fraud, the UK's national fraud and cybercrime reporting centre. Reporting helps build intelligence and can prevent others from becoming victims.

If you are affected by the content of this bulletin, you can talk to us. Our Scams Awareness and Aftercare Team can offer free support, advice and guidance. Contact our team today on:

☎ 01625 612958 (OPTION 5)

✉ scams@ageukcheshire.org.uk

A simple three-step rule

When it comes to QR codes, remember:
Pause – Check – Go Direct

- Pause before scanning
- Check for tampering or suspicious wording
- Go direct to official websites whenever possible

Technology itself is not the enemy. QR codes are simply tools. But like any tool, they can be misused.