

The Emerging Threat of QR Code Scams: Understanding and Preventing "Quishing" Attacks

Between April 2024 and April 2025 there were 784 reports of "quishing" (QR-code phishing) to UK police reporting service Action Fraud. These scams led to losses of £3.5 million. Action Fraud (2025).



Executive Summary

QR codes have become an everyday convenience, enabling instant access to websites, mobile payments, app downloads, and contactless services. However, the very simplicity that makes QR codes so useful also makes them a potent tool for cybercriminals. A new wave of scams—often called “quishing” (QR phishing)—exploits this technology to trick users into revealing personal or financial information, downloading malware, or making fraudulent payments.

One of the most common and dangerous forms of this scam involves fake parking or payment QR codes, where fraudsters replace or overlay legitimate codes on parking meters, charging stations, or public signage. Unsuspecting users, believing they are paying for a service, are redirected to a fraudulent website and unknowingly hand over sensitive details.

This whitepaper explores how these scams work, the risks they pose to individuals and businesses, and the strategies needed to reduce exposure.

1. Introduction

QR codes (Quick Response codes) have evolved from niche technology into mainstream tools, especially since the COVID-19 pandemic accelerated the shift toward contactless interactions. They are now widely used for:

- Restaurant menus and ordering
- Event check-ins and ticketing
- Parking and transport payments
- Public health campaigns
- Business marketing and promotions

Global adoption has made QR codes familiar, trusted, and convenient. Unfortunately, cybercriminals exploit this trust, knowing that most people scan QR codes without a second thought.

In 2025, QR codes have become both a symbol of convenience and a growing cyber battleground. Once seen as harmless shortcuts to menus, payments, or check-ins, they are now being weaponized in increasingly sophisticated ways. Attackers use “quishing” (phishing via QR codes) to lure victims into fake login pages, payment portals, or malware downloads, often by pasting counterfeit stickers over legitimate codes or embedding cleverly split and nested QR images that bypass filters and look genuine to the eye. The danger lies in the fact that you can’t see the destination until after scanning, and by then a single tap can hand over your data, install spyware, or redirect funds. With QR use exploding in public spaces, retail, and finance, these threats are spreading faster than most defenses can keep up. The good news is that awareness and simple habits can dramatically reduce the risk: check the source of a QR before scanning, use apps that preview links, and never allow unnecessary permissions like WiFi auto-join or app installs. For businesses, branding QR codes, securing generation with HTTPS, and training employees against quishing are becoming as essential as email security. In short, QR codes remain incredibly useful—but in 2025, every scan should come with a quick moment of caution, because that “convenient square” could be a cyber trap in disguise.

2. The Anatomy of a QR Code Scam

Unlike phishing emails or suspicious links, QR code scams are harder to detect because the information they contain is hidden until scanned. Common techniques include:

a. Fake Parking/Payment QR Codes

- Fraudsters print realistic QR code stickers and place them on parking meters, EV-charging stations, or payment kiosks.
- Scanning the code redirects victims to a spoofed payment page, often resembling a council, utility, or vendor site.
- Victims enter card details or pay, believing they are completing a legitimate transaction.
- Criminals harvest financial data or divert funds directly to fraudulent accounts.

b. Package and Delivery Scams

- Unsolicited packages arrive with enclosed QR codes, urging recipients to "scan to see who sent the gift" or "confirm delivery."
- Scanning directs users to malicious websites or installs malware.

c. Social Engineering and Messaging

- Text messages or emails include QR codes claiming urgent action is needed (e.g., "Your parcel is waiting" or "Pay now to avoid a fine").
- Scanning bypasses suspicion that might arise if a suspicious link were displayed outright.

d. Sticker Overlays

- Fraudsters apply adhesive QR stickers on top of genuine codes on posters, transit signage, or advertising boards.
- The altered code routes users to phishing websites instead of the intended destination.



3. Why This Scam Works

Several psychological and technical factors make QR scams effective:

1. **Visual trust**, QR codes look neutral, not inherently suspicious.
2. **Hidden content**, URLs are not visible until scanned, unlike email links.
3. **Urgency & authority**, Phrases like “pay now” or “scan to confirm” exploit the human tendency to prioritise urgency.
4. **Ubiquity**, QR codes are everywhere, from parking meters to health check-ins, normalising their use.
5. **Low cost for attackers**, Printing stickers or embedding a malicious QR code requires minimal resources.

Visual trust

QR codes look neutral and technical. People do not associate them with fraud in the same way they do suspicious emails or pop-ups. A small black-and-white square carries an appearance of legitimacy. Attackers exploit this by placing malicious QR codes on posters, invoices, or even menus in restaurants. A victim scanning the code sees only a neat pattern, not a phishing link.

Hidden content

Unlike an email link, where you can hover and preview the URL, QR codes hide their destination until scanned. This gives attackers an advantage. A malicious QR code can redirect to a fake banking login page, a malware download, or a fraudulent payment portal. Victims often realise too late. For example, Action Fraud reported cases where drivers scanned parking meter QR codes that redirected to cloned payment websites, stealing both card details and personal data.

Urgency and authority

Fraudsters often pair QR codes with urgent instructions. Messages like “scan now to avoid penalty” or “confirm payment immediately” create pressure. People under stress skip verification. In one reported scam, UK residents received fake letters from energy providers with QR codes directing them to “confirm account details” to avoid service suspension. The authority of the brand and the urgency of the message made the fraud effective.

Ubiquity

QR codes have become part of daily life. They appear in cafes, gyms, offices, car parks, and healthcare facilities. This constant exposure normalises scanning without question.

During the pandemic, QR codes were used for health check-ins and vaccination bookings. Criminals took advantage of this trust by placing fake QR codes near official notices, knowing that people expected them and rarely questioned their authenticity.

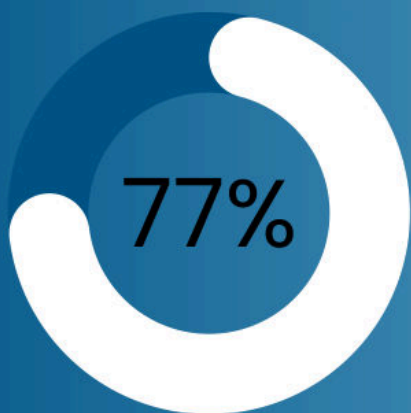
Low cost for attackers

Running a QR code scam is cheap. A fraudster only needs to generate a code online, print stickers, and place them strategically. Compared with sophisticated malware campaigns, this requires almost no technical skill or infrastructure. In one case, attackers placed fraudulent QR codes on EV charging stations, tricking drivers into entering payment details on fake sites. The total investment for the attackers was minimal, yet the potential reward was significant.

4. Risks and Impacts

The consequences of falling victim to a QR scam can be severe:

- **Financial Loss:** Fraudulent transactions, unauthorised card charges, or drained accounts.
- **Identity Theft:** Harvested personal data (names, addresses, ID numbers, logins) used for fraud.
- **Reputational Damage:** Businesses whose signage is exploited risk losing customer trust.
- **Malware Infections:** Malicious links can trigger spyware or ransomware downloads.
- **Operational Disruption:** For municipalities or companies, widespread scams at parking or charging stations can undermine service trust.



Reports of QR code fraud in the UK grew by 77% year on year from 784 cases in 2023/24 to 1,386 cases in 2024/25 (Action Fraud, reported by The Guardian, 2025).

5. Real-World Examples

Parking Meters in the UK and US

Police and councils have warned drivers about fake QR stickers placed on parking meters, directing victims to fraudulent payment portals.

Phishing Campaigns in Corporate Settings

Employees received QR codes embedded in fake “account reset” notices. Scanning led to credential theft.

Consumer Packages

The FBI has warned about unsolicited packages that include QR codes, linked to malicious websites.



6. Prevention and Protection

To mitigate the risks posed by QR scams, both individuals and organisations must adopt proactive measures:

For Individuals

- Verify the source: If possible, use official apps (parking, delivery, banking) instead of scanning public QR codes.
- Inspect physical codes: Look for tampering—peeling stickers, misaligned labels, or codes placed over existing signage.
- Preview URLs: Many phones allow you to preview a QR code's destination link before opening it. Check for HTTPS and correct domains.
- Be sceptical of urgency: Treat "scan now or lose access" messages with caution.
- Report suspicious codes: Notify local authorities, building managers, or your bank if you encounter or fall victim to a scam.

For Businesses

- Secure signage: Regularly inspect public-facing QR codes on meters, kiosks, and posters.
- Educate customers: Post warnings that official services never require QR scans for payment unless through verified apps.
- Monitor branding: Ensure logos and trademarks aren't being used in spoofed websites linked to fake QR codes.
- Deploy safer alternatives: Encourage NFC payments, dedicated apps, or machine-integrated payment systems rather than static codes.



7. Conclusion

QR codes are here to stay, offering convenience and efficiency in an increasingly digital society. However, they also represent a growing attack vector for cybercriminals. The new wave of QR code scams—particularly fake parking and payment codes, demonstrates how attackers exploit trust, urgency, and hidden content to commit fraud.

Awareness, vigilance, and proactive defence are key to reducing risk. By educating the public, hardening business processes, and developing smarter safeguards, society can continue to benefit from QR code technology without falling prey to its darker side.

References & Further Reading

- Action Fraud (2025) QR codes. Action Fraud.
- The Guardian (2025) QR code scam reports more than double in a year.
- FBI Public Service Announcement (2025): QR Code Package Scams.
- The Guardian (2024–2025): Reports on fake parking QR codes and quishing scams.
- Third Federal: Security Advisory on QR Code Scams.
- UK Police Cyber Crime Units: Public warnings on parking meter scams.

Join Our Social Community

