



Emerging Threats - QR Code Scams Playbook: A New Frontier in Cyber-Fraud

JUNE 2, 2025 - Threat Intelligence Team

QR Code Threat Actor Tactics: The Fraudster's Playbook

QR codes have become a convenient bridge between the physical and digital worlds, offering quick access to payments, websites, and services with a simple scan via a smartphone. The widespread adoption of QR codes, particularly in parking and transport systems, has made them an attractive target for cybercriminals. By exploiting public trust and the time pressures faced by motorists, scammers are physically embedding malicious QR codes into everyday environments in attacks known as quishing or QR code phishing. This piece explores how these attacks unfold and strategies to prevent, detect, and respond to this growing threat.

Step 1: Cybercriminals Register a Phishing Website or Premium Number



Summary:

The attack begins with criminals setting up or repurposing a fake domain or a premium-rate number. The site is designed to resemble a legitimate parking or financial service to trick users into entering sensitive data or initiating contact.

- **Risk Origination:** Registrar, Premium Number Vendors
- **Prevention:** Registrar vetting for suspicious domains; AI-driven website fingerprinting to detect fake versions of known services. Proactive daily alerts anytime a suspicious domain similar to a parking operator's domain is registered.

- **Detection:** URL-scanning services, AI for domain similarity detection, proactive daily indexing/investigation of suspicious or newly registered domains mimicking trusted parking operators.
- **Education:** Engage registrars in improving KYC controls and implementing stricter checks for unfamiliar domains. Promote the use of official apps.

Step 2: Parking Machines Are Physically Compromised and Overlaid



Summary:

Criminals physically place QR code stickers over legitimate ones on parking meters or public kiosks, redirecting users to phishing pages.

- **Risk Origination:** Parking Management Company, Car Park Physical Security.
- **Prevention:** Tamper-proof stickers, digital authentication of QR codes, hardened machine design.
- **Detection:** Automated hourly inspection using computer vision cameras for QR code-domain verification; parking machine CCTV; anti-tamper parking payment machines.
- **Education:** Public advisories encouraging users to double-check URLs after scanning and visible reminders throughout the car park.

Step 3: Motorists in a Hurry Scan Fake QR Code on Parking Machines and Enter Details



Summary:

In a rush, motorists scan the malicious code or phone a premium number, unknowingly submitting sensitive information or card details to fraudsters.

- **Risk Origination:** Motorist, Parking Management Company.
- **Prevention:** Default mobile OS settings to preview and risk assess links; on-site attendants or security patrols at car parks to deter cybercriminals.
- **Detection:** On-device security, QR code scanner apps with anti-phishing detection, and anti-vishing technology.
- **Education:** Campaigns focused on slowing down digital interactions, "*Think Before You Scan*" awareness materials.

Step 4: Cybercriminals Impersonate the Target's Bank Through Calls, SMS, or Emails



Summary:

With stolen data, attackers impersonate banks via spoofed communication to induce urgency and extract further information or payment.

- **Risk Origination:** Banks; Mobile Network Operators (MNO).
- **Prevention:** SMS firewalls, number spoofing detection, SIM-swap detection, vishing detection and anti-impersonation protocols.
- **Detection:** Stronger customer end-to-end journey and customer security for bank customers; anti-fraud products flagging language patterns in SMS/email using NLP.
- **Education:** Teach users that banks never ask to transfer funds; simulate attacks for training; publicize recent scam cases.

Step 5: Victim Panics and Transfers Money to a "Safe Account" (APP Fraud)



Summary:

In a final blow, victims are manipulated into transferring money under the guise of protecting it, resulting in APP fraud - often irreversible.

- **Risk Origination:** Banks.
- **Prevention:** Banks implementing Confirmation of Payee checks, develop customised risk scores and profiles for each customer and multi-step authentication for "urgent" transfers that aim to transfer a cumulative total of more than 80% of the customer's account balance.
- **Detection:** Real-time fraud analytics, pattern recognition, and cross-bank collaboration to spot unusual flow of funds into bank accounts.
- **Education:** Empower users to resist pressure as part of onboarding processes when a new customer opens an account; debunk "safe account" myths; warn about urgency as a red flag and create learning pathways and training programmes for all customers.

Conclusion

The increase in QR code attacks, QR code phishing, also known as quishing, is a prime example of how physical and digital vectors merge to create sophisticated fraud that leads to financial losses and identity theft. Addressing this complex attack requires a multi-layered security strategy combining:

- Physical Security
- Anti-Tamper Measures
- Cyber Security
- Proactive Detection
- On-site Automated Detectors Using Computer Vision to Identify Scam QR Codes
- Security Awareness Campaigns

In each of the five steps we've identified in this article, there were several prevention, detection, reporting, and education opportunities that could be leveraged. To reduce the risk to potential targets and to prevent fraud - car park operators, local authorities, banks, law enforcement, mobile network operators (MNOs), and domain registration companies all have a part to play in collectively strengthening physical, hybrid and cyber security in areas susceptible to QR code scams.

PROFILE: PORGiESOFT Security provides advanced fraud intelligence, scam listening, analysis of emerging cyber threats and other anti-fraud cyber security products and services. Our vision is to be a world-class leading authority in the detection and prevention of cyber-fraud, inspecting language as data.

PORGIESOFT LTD

PORGIESOFT LTD is a company registered in England and Wales. Registered Number: 11660739

Registered Address: Future Business Centre, King Hedges Road, Cambridge, United Kingdom. CB4 2HY

PORGIESOFT SECURITY is an anti-fraud cybersecurity firm based in Cambridge, with our team working around the world. We're an NCSC (a part of GCHQ) for Startups Alumni Startup. We specialise in fraud intelligence - combining research data, threat intelligence (phishing, smishing), OSINT, transaction analytics and artificial intelligence to prevent fraud, helping consumers, employees, and businesses stay safe online.

