Taking on the scammers

Amidst a surge in reports of QR code scams and bogus PCNs, *Parking News* investigates how operators can protect both themselves and their customers

WORDS | ANDREA BALL

"The UK is experiencing a fraud and scams emergency." That's the warning from Simon Miller, director of communications at the fraud prevention service Cifas. According to Citizens Advice, nine million people had been caught out by financial scams in the year up to October 2024. While many of those have fallen victim to fake debt advice or investment fraud, up to 2.5 million people are thought to have been affected by parking scams.

In addition to QR code scams, fraudulent apps and bogus penalty charge notices (PCNs) have also been used to trick motorists and there have been reports of incidents across the UK. In October 2024, Action Fraud told BBC Radio 4's consumer programme *You and Yours* that it had received 2,600 reports mentioning the word 'parking' so far that year – double its figures from 2022.

QR code scams, dubbed 'quishing' (QR phishing), involve scammers placing stickers with bogus QR codes over genuine codes at car parks. Scanning the bogus code can sign consumers up for subscription payments without their consent, or direct them to fake payment websites where their personal and financial information is stolen.

The fake PCN messages include a link to a very convincing copycat Government website complete with accurate fonts, branding and logos, but any payments made end up with the fraudsters. Often, there are three successive messages: the first informing the consumer of the fake parking charge, the second telling them they must pay, and a third threatening them with legal action or a driving ban if they don't pay. The links in the messages are often hosted by a QR code generating website, so people are also at risk from automatic, recurring payments being set up on their accounts when trying to pay what they believe is a parking fine.

"Criminals are using a catalogue of fraudulent tactics to target high volumes of consumers with ease, and on a vast scale," explains Simon. "Scammers are constantly adapting their methods to exploit innocent people and will prey on the services and products that consumers use day in day out. Parking is no exception.

"The wide availability of fraud toolkits and AI online means that it is all too easy for criminals to recreate high-quality

Tamper-proof QR codes

FAAC Mobility Services (FMS) has developed tamper-proof 3D printed QR codes to address the problem of QR code fraud. Built to withstand environmental conditions, the QR code is embedded into the physical structure of the parking sign, making it much harder for fraudsters to tamper with or replace the codes without being detected.

During a three-month trial at the Centrale and Whitgift Shopping Centre in Croydon, there were no reported cases of QR code tampering, and users reported having more trust in the system. Operators also reported having fewer maintenance issues and reduced costs associated with replacing tampered QR codes.

legitimate websites, and spoof emails or social media content that impersonate genuine brands and apps."

Mark Wilson, chief commercial officer at Unity5, provider of the Zatpark platform, agrees that the increase in fraud has been exacerbated by our increasing reliance on digital payment systems. "The evolution of payment methods, among other emerging technologies, has enabled scammers to take advantage of some consumers," he explains. "While these payment types bring security and reliability to motorists and operators, scammers have found ways to exploit the point of payment for fraud, increasingly via QR codes."

Safety campaign

Sean Green is the parking manager for Westmorland and Furness Council in Cumbria, which is launching an annual campaign, Pay Smart, Pay Safe, to coincide with the busy summer period. "It's very important to make customers aware of the dangers," he explains. "Simple things like advertising which apps you use and how to use them safely can help."

The council is advising people to only download payment parking apps from official app stores, such as Google Play Store or Apple App Store, and to pay close attention to any websites they are directed to, to ensure they are genuine.

"The campaign will give practical advice about our providers, how to use them safely, and how to spot fake websites, as well as what to do if you are a victim of fraud," says Sean. "We also carry out regular checks in the car parks to ensure the signage has not been tampered with.

"I would encourage all operators to talk to their cashless payment providers regularly to find out what they are doing to combat the threat to customers and ensure they are kept up to date with the latest scams and solutions to beat them."

Advice for operators

Some parking app providers have taken the decision not to use QR codes, but Unity5 is advising those that do to use dynamic, hi-res QR codes and place them in open, well-lit areas that are visible and easily accessible, reducing the risk of them being covered or tampered with. Larger QR codes are harder to cover discreetly, and high-quality printing reduces wear and tear, making tampering more noticeable.

"Educating users is equally important," adds Mark. "We're providing templates and updates to support customers through signage and digital communications. Operators should inform users about the potential risks of QR code tampering and encourage them to report any suspicious activities."

Finding a balance

It can be a challenge for operators to enhance safety features while ensuring an accessible experience for motorists. Unity5 believes that the key to finding that balance is an increased focus on monitoring, and suggests using parking enforcement software to schedule frequent inspections of QR code stations.

"We've developed a Task Management tool in our app which supports checking and removing fraudulent QR codes," Mark explains. "Administrators can use this tool to set up reminders for their CEOs to check and photograph signage on site as well as to log any fraudulent activity."

Raising awareness

Simon says Cifas is urging consumers to remain vigilant to parking scams and wants the industry to ensure people are aware of the risks. "Always question something that doesn't look right or seems too good to be true, and report anything suspicious," he says. "It's also vital that parking providers continue to raise awareness of this issue so that fraudsters can be tackled at the earliest opportunity."

The BPA has launched its #ParkAware campaign to do just that. Sarah Greenslade, BPA content and research manager, says: "We encourage all members to support our fraud prevention #ParkAware campaign. It is essential we are vigilant, adhere to best practice and educate motorists about the risks and the importance of reporting scams. If we work together as a sector we can prevent it happening."

Cifas provides five tips to share with customers

- Only use official apps from trusted app stores. Be cautious of third-party sites or emails that request you to download links.
- Don't click on unsolicited links or hand over sensitive information, such as your bank details, to someone you don't know or trust.
- Report scam websites to the National Cyber Security Centre at: report@phishing.gov.uk and forward texts to 7726 – a free service that allows mobile customers to report suspicious texts and calls.
- If you've been the victim of fraud or a scam, contact Action Fraud at: www.actionfraud.police.uk or call 0300 123 2040 (in England, Wales or Northern Ireland). Call the police on 101 if you are in Scotland.
- If you've been a victim of identity theft or fraud, pay to protect your identity through Cifas' Protective Registration service: www.cifas.org.uk/pr

Useful resources
BPA has put together a dedicated web page to help members inform the public on how to avoid being scammed, as well as an asset pack to use on social media. Don't forget to share the campaign by using the #ParkAware hashtag.

Asset pack

Member guide: Preventing parking payment fraud

Public advice web page