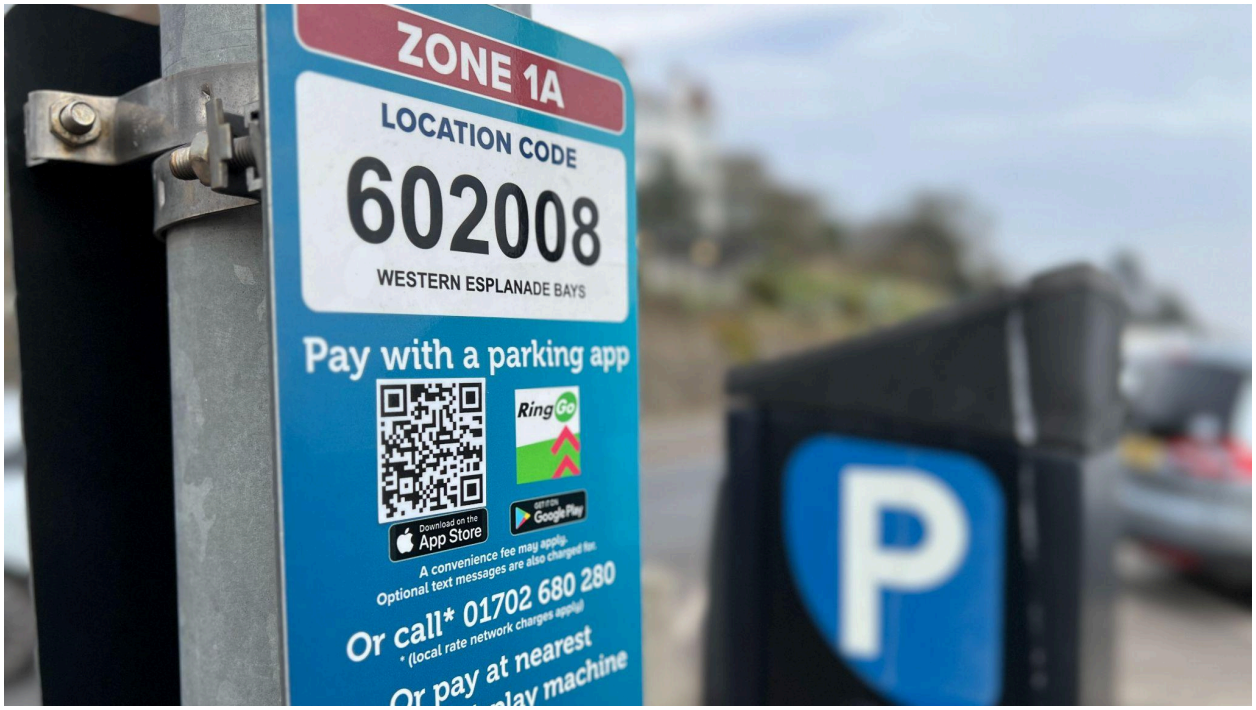
LOCAL NEWS PARTNERSHIPS



QR code scams

Embargoed - 11 April 2025

Please note this report and accompanying dataset is subject to change

BBC Shared Data Unit, BBC Local News partnerships

shared.dataunit@bbc.co.uk

The Drum Online Media Awards
Winner 2020

Contents

What's the story?

The number of scams linked to QR codes has soared more than tenfold across the UK in just five years, the BBC has found.

Since 2019, thousands of people have been tricked by fraudsters using QR codes to steal money and personal information.

Organised gangs are often behind the fast-spreading crime, according to Katherine Hart, lead officer at the Chartered Trading Standards Institute.

She said so-called 'quishing' is significantly underreported and is presenting a "huge challenge" to authorities globally.

"We've seen huge amounts of money lost this way, people have seen their life savings gone and that money is going to finance criminals," Ms Hart added.

Quishing scams usually see misleading QR codes created by criminals placed where contactless payments are common, such as on parking meters or restaurant menus. They have also been spotted on packages, in emails and on television.

The malicious codes redirect users to fraudulent websites or applications and can be used to extract personal data, such as bank details.

The BBC's Shared Data Unit obtained Action Fraud data that shows nearly 3,000 reports linked to QR codes were reported to the national fraud reporting centre between 2019 and 2024.

Last year, 1,386 reports were logged - more than double the 653 in 2023 and significantly higher than the 100 reported in 2019.

The accompanying data will allow you to see how the scam has grown in your police force area across the UK.

The BBC has reported on dozens of examples of people around the country falling victim to QR code scams in recent years.

Councils including Luton, Guildford, Reading, Bournemouth, Christchurch and Poole, West Northamptonshire, Trafford, Aberdeen, Sussex, Cheltenham, Flyde, Stroud, Southend on Sea, Leicester City, Conwy, Telford and Wrekin, Kensington, Southampton, Coventry and Shropshire are among those to have issued warnings.

What is a QR code?

- QR stands for ‘quick response’
- QR codes look like black and white squares
- They work like a two dimensional bar code and can be scanned by a phone or tablet
- Businesses often use them legitimately to direct users to apps, payment platforms, social media accounts, menus and events listings

Ms Hart said the true scale of the problem is far higher as many do not report being targeted,

She said victims often lose small amounts of money initially, as those responsible gather the data they need to launch a “secondary scam”.

“You might lose £2.99 and a lot of people won’t report that and don’t realise they’ve passed on their information to a criminal organisation,” Ms Hart said.

“Invariably, days or weeks later they’ll get a call telling them they’ve been the victim of a fraud and they can pinpoint a day, because they already have all of this information you’ve shared with them earlier.

“They convince you using very coercive tactics that they’re from your bank, police or Trading Standards and they want access to your bank account to take everything you’ve got.”

Experts including the national fraud reporting service ActionFraud and the National Cyber Security Centre (NCSC) say it is “vital everyone stays vigilant” to cyber criminals.

A NSCS spokesman added: “When directed to a website by a QR code - especially in open spaces like stations or car parks - it is important to take care to ensure that it is genuine, and be cautious if you're asked to provide excessive personal information.”

Other stories include:

- A Thornaby woman who lost £13,000 trying to pay for parking at a railway station
- Fake QR codes in North Northamptonshire
- A driver who lost £170 at a seafront car park in Sunderland
- A man tricked into paying £39 to park his motorhome in Skegness
- Bogus codes with links to Russia found in Leicester
- Greater Manchester Police issue QR code warning

About the data

The BBC's Shared Data Unit analysed five years' worth of data provided by ActionFraud, the national fraud reporting centre.

The data, which represents the number of reports made to ActionFraud, is broken down by police force area and by year.

ActionFraud is a self-reporting service and the statistics are based on reports and information provided by the public via an online self-reporting tool.

A spokeswoman for ActionFraud said information provided within the reports may not have been verified by police or interrogated for authenticity or accuracy and may therefore be subject to discrepancies.

How to use this pack

Separate to this document we have provided you with a spreadsheet containing all of the data for police force areas across the UK.

Police force areas are ordered in alphabetical order in the sheet by default.

We recommend you find your area using the find function (Ctrl and F).

Please take time to read the column headings carefully when compiling your report.

What we found

Our study looked at data linked to 45 individual police forces in England and Wales, and to Police Scotland and the Police Service of Northern Ireland (PSNI).

Headline figures

- **2,922** QR-code related scams were reported to ActionFraud between 2019 and 2024
- The number of scams has risen every year, going up more than ten-fold from **100** in 2019 to **1,386** in 2024
- Year on year, the number of scams more than doubled between 2023 and 2024, rising from **653** to **1,386**
- **2,608 - 89% -** of the scams were linked to forces in England and Wales
- 60 were linked to Police Scotland and 47 to PSNI
- One in five of the scams recorded across the UK (21%) were linked to the **Metropolitan Police** force area

Quotes and expert comment

Katherine Hart, lead officer for the Chartered Trading Standards Institute on doorstep crime scams and consumer vulnerability, said:

“The figures do not reflect the scale of the problem because the nature of this fraud means it often goes unreported.

“Sometimes that’s down to consumer embarrassment but a lot of the time we’re just not sure how to report or record them.

“People aren’t sure where to report the frauds to and at the end where they’re taking the details, it can be difficult to know what to record this as - is it a parking scam? A banking scam? A delivery scam?

“There are a huge amount of challenges facing the authorities as we don’t know where these scams are.

“At the end of the day they do tend to be run by serious and organised crime groups.

“They are so sophisticated and this is massive now, it’s a global issue.

“But those putting up fake QR codes are sometimes just paid a small amount of money and often won’t have a clue what they’re doing.

“That’s the nature of organised crime groups, there’s a hierarchy of structure and sometimes the ones committing the crime have no idea.

“Parking meters were just the start, we’re now seeing QR codes posted everywhere, from within emails to texts and through the post.

“They take you to a platform that’s designed to take our details, where the criminal can scam you on the spot and take your money or data harvest to use your details later down the line, which is a worrying thing.

“Quite often, the codes will take you to a payment platform and people pass on lots of personal detail and their credit card or bank details.

“You may lose £2.99 or £5.99 and a lot of people won’t report that and don’t realise they’ve passed their information to a criminal organisation.

“Invariably, a couple of days, weeks or even months later, they’ll get a call telling them they’ve been a victim of fraud and they already have all of your information because you’ve shared it with them earlier.

“They convince you using very coercive tactics that they’re from your bank or police or trading standards.

“They want access to your bank account to take everything you’ve got.

“On average, people lose £2,000 to banking scams but we’ve seen huge amounts of money being lost in this way.

“People have seen their life savings gone and at the end of the day, that huge amount of money is going to finance those criminals.”

Detective Superintendent Gary Miles, head of the National Fraud Intelligence Bureau at the City of London Police, said:

“We know that QR codes can be used in all aspects of life, online and in-person, however this doesn’t stop fraudsters finding new ways to target members of the public.

“With the rise of reports in mind, we encourage everyone to stay alert to QR codes that could be fraudulent.

“You should stop and check before scanning one: if you’re in-person, check for signs it has been tampered with, or online, look out for phishing emails or rogue social media posts with QR codes.

“If you scan a QR code and it takes you to a website you feel doesn’t look right, do not share any personal or financial information, and leave the website immediately.

“If you’ve been a victim of fraud, report to your bank immediately and report to Action Fraud online at actionfraud.police.uk or by calling 0300 123 2040.
“In Scotland, call Police Scotland on 101.”

A spokesman for the National Cyber Security Centre said:

"With more businesses using QR codes to direct people online, it is vital everyone stays vigilant to cyber criminals who might try to exploit this.

"When directed to a website by a QR code - especially in open spaces like stations or car parks - it is important to take care to ensure that it is genuine, and be cautious if you're asked to provide excessive personal information.

"By staying alert online and following practical steps available on the Stop! Think Fraud website, individuals can help protect themselves from falling victim to cyber crime."

A spokesperson for the National Crime Agency said:

“Fraud is the most prevalent crime in the UK, and one that causes victims long-lasting emotional and psychological harm as well as financial loss.

“Much of the most harmful fraud impacting the UK is committed by organised criminals, often based abroad.

“We are working closely with partners, both law enforcement and private sector, across the world, to tackle the threat.”

A spokesman for National Car Parks (NCP) said:

“NCP is very vigilant to the threat of fraudulent QR codes which could affect our customers and our business.

We have made sure that we have a rigorous process in place which works to try to prevent anyone being able to compromise our use of QR codes.

“We have limited data as a business on this as it is a very rare occurrence to date, and we are working hard to keep it that way.

“We have had a couple of incidents where we have been made aware that a customer has used a QR code in a car park which has been placed over our original QR code, which has led them to a fraudulent payment page.

“With this in mind we ask our teams to monitor the signage for all our QR codes on a daily basis, and we also ask them to physically scan the codes to ensure that no one has placed a false QR code as an overlay.

“As a business that has multiple machinery and signage with our QR codes displayed, all of which are open to the public, we are very aware of this issue.

“To summarise, to date we have had reports from customers on two sites only and have immediately issued further notices to our teams to check all QR codes themselves on a daily basis.

“We welcome all initiatives to remind the public to be vigilant when using QR codes. To further mitigate against fraudulent QR code activity, we are currently reviewing options to reduce the impact on our customers.

“This could include removing a QR code from our signage that directs customers to a payment page, and instead emphasising the use of our website. We understand the value of QR codes and will still look to use them where we can safely.”

Police Service Northern Ireland (PSNI) said:

The Police Service of Northern Ireland is warning the public of the increase in QR code scams, particularly as more people use them for check-ins, accessing online links and even to place food orders at restaurants, bars and cafes.

Detective Chief Inspector Uel Boyd, the PSNI lead on Economic Crime, said: “Use of these codes is becoming more and more common as it directs users to websites. With this popularity, we’ve seen an increase in scams operating in this space. These QR code scams operate similar to conventional phishing tactics, where perpetrators conceal malicious links within QR codes, and QR code phishing also known as ‘quishing’ will be a scam to watch out for.

“We’d advise the public to be aware of compromised QR codes in public, such as car park meters, restaurants and signs for free public Wi-Fi. Double check that a legitimate code hasn’t been tampered with, and there is not a sticker placed on top of another QR code.

“Look for typos and spelling mistakes in the website address. Be cautious if asked to give access to your phone, computer, location, microphone, or any other features on your devices after scanning the QR code.

“Don’t share personal or financial details after scanning a QR code, as it is likely a scam.”

For more information on how to avoid being scammed visit:
https://www.psni.police.uk/safety-and-support/keeping-safe/scams-and-fraud

To report this or any type of fraud, report to police on 101, to your bank immediately, online at www.actionfraud.police.uk or call 0300 123 2040.

Information and advice is also available at http://www.nidirect.gov.uk/scamwiseni or the ScamwiseNI Facebook page @scamwiseni

Wayne Stevens, National Fraud Lead at Victim Support, said:

“In the last five years, there has been a huge increase in the number of businesses and organisations using QR codes to share information with the public.

“Unfortunately, this has also given criminals the opportunity to target people using more and more sophisticated schemes.

“When scanning a QR code, it is important that people ensure the code does not appear altered or distorted in any way, and the destination URL is as expected.

“There is a lot of embarrassment, shame and stigma associated with cyber fraud, but it is vital that victims do not blame themselves. If you have been impacted, contact Victim Support for free, confidential support.”