scam share

spotlight on...

QR Code Scams

Scanning a scam QR code could lead to a malicious website that gathers your details. It could allow scammers to access functions/apps on your phone.

QR Codes are square barcodes that a smartphone camera can scan and read to provide quick access to a website or app.

Common Scams

An email that appears to be from HMRC and asks you to scan a QR code to update your personal information or make a payment

(QR codes used in genuine correspondence from HMRC will ONLY lead to guidance on GOV.UK. They will never lead to a page where you are asked to enter personal or payment details)

Scammers sticking their own QR codes on top of legitimate ones in car parks and at electric car charging points

Scammers sticking their own QR codes on top of legitimate ones on posters and adverts in public places

Avoid QR Code Scams

Never scan a QR code from an unfamiliar or unexpected email

If the message appears to have been sent by a company or organisation, visit their legitimate website to make a payment or update details rather than scanning a code

If you are paying for parking or car charging, visit the website listed on the payment machine or charging point rather than scanning a QR code

Where possible, and especially in public places, check for visual indications that a QR code has not been tampered with

Review the preview of the QR code's URL before opening it

You can do this by opening your mobile device camera and pointing it at the QR code. This will provide the site address the code will take you to. Make sure the website uses HTTPS rather than HTTP, doesn't have obvious misspellings and has a trusted domain. Don't click on unfamiliar or shortened links.

Be wary if a QR code takes you to a site that asks for personal information, login credentials or payment

Scam messages will often have a sense of urgency and will appeal to your emotions to try and convince you to take action quickly

Report QR code scams

Report all scams to **Advice Direct Scotland** on **0808 164 6000** or via **scamwatch.scot**
You can forward suspicious emails to **report@phishing.gov.uk**
If you have lost money or are worried that you have given your bank details to scammers, **contact your bank and report it to Police Scotland on 101**

Find out more:

www.tsscot.co.uk/scamshare