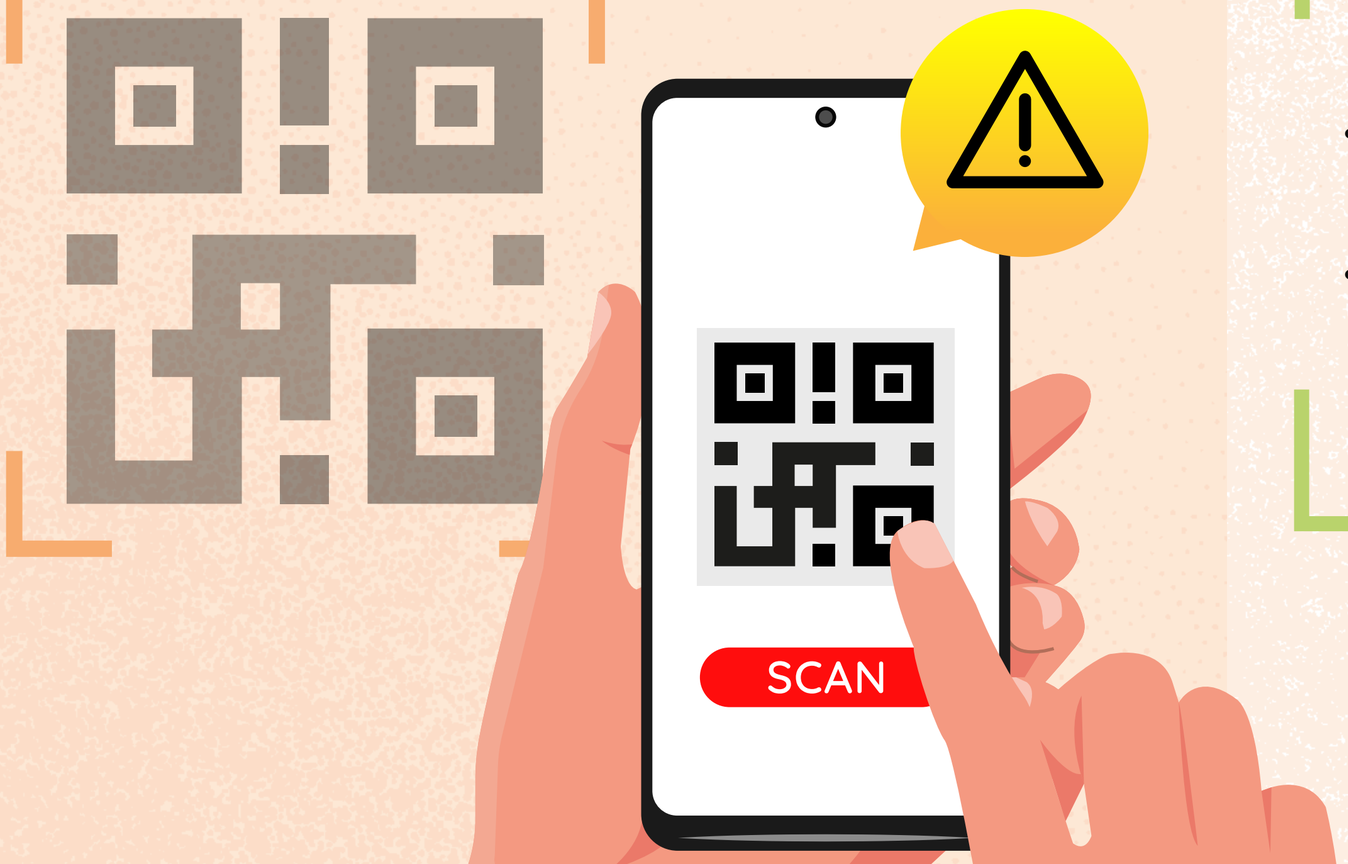
QR CODES
HOW TO AVOID A SCAM...

We're familiar with QR codes now in our everyday life for products and services. From purchasing tickets or ordering food at restaurants, to paying for parking or just connecting to Wi-Fi...they have become a part of our lives for quick and easy access to websites.

QR (Quick Response) codes are like barcodes. When we scan them with a mobile phone camera, a link to the information they hold appears. Whilst providing us with a quick and easy way to access information, not all of them are secure. Cyber criminals can use QR codes to steal personal and bank details.



However, there are ways to protect yourself from this fraud.

QR phishing, also known as 'quishing' uses malicious QR codes to send users to a fraudulent website or prompt a download of harmful software that spreads malware or prompts the sharing of confidential information.

- Cyber criminals posing as real companies send phishing emails with a QR code and ask users to scan it. Then, they attempt to obtain information or spread virus-infected files.
- Another common scam is the false QR code stuck on top of an original one, like in restaurants or street advertising. False QR codes can even be found on parking meters, linking to a credible but fake payment site to steal money or credit card information.
- Scammers using inverted QR codes firstly create a malicious code and then use it as a presumed payment method. But the code does exactly the opposite: it requests money from the user. This type of scam is also used to steal personal information and bank details.

How to avoid a QR scam

- Before scanning a QR code, like in a restaurant or a public space, check that it hasn't been tampered with or got a sticker placed over an original code.
- Installing anti-virus software for your device will help you avoid having a virus or other malware downloaded onto your mobile.
- Check the preview of the QR code link. When you scan a QR code, a preview of the URL should display on your device. Make sure the website address is legitimate. Look for a padlock symbol and an address that begins with "https://". Only those URLs are secure.
- Think twice if the app or website you're being directed to ask you to provide personal details. If it does, make sure it's authentic.
- Scanning QR codes in open spaces (like stations and car parks) might be riskier. As with many cyber attacks, you should be suspicious if you're asked to provide what feels like too much information, whether that's on a website or in any follow-up communications (such as a phone call).