QR CODES

Scams using fake QR codes are on the rise. Here are some known scams.

QR code scams on parking meters and other contactless payments

One of the most common uses of QR codes is to enable customers to quickly pay for goods and services, such as meals or parking. But any QR code placed in public offers a prime opportunity for a scammer. Scammers can put their QR codes over genuine ones. When unsuspecting victims scan the QR code, they are sent to an official-looking payment page to pay for parking. But when they entered their credit card information, it is sent to scammers who could then use it to make fraudulent purchases or even sell the victims' personal data.

Fake QR codes sent in phishing emails

Be cautious of any QR code that is sent in an email.

These scams typically entail receiving an unsolicited email that contains a QR code needed to "view" a document, invoice, picture, or something else that is enticing to the recipient.

For example, scammers will often send "failed payment" emails that include a QR code.

These scams claim to come from a retailer you trust, like Amazon. The email will claim that a recent purchase of yours didn't go through and that you need to scan the QR code to complete the transaction.

But again, if you enter your credit card information, it will go straight to the scammer.

As a general rule, don't scan QR codes that are sent to you in emails. If you think an online purchase didn't go through, log into your account directly on the company's website instead of using a QR code.

Fake QR codes sent by post

Scammers will sometimes send physical mail containing QR codes claiming to offer giveaways, prizes, or instant coupons. But these are very often scams.

Regard physical junk mail the same as you would spam emails in your inbox. If you don't know the sender personally, don't click on (or scan) any links. If it is a legitimate company offering a discount or special offer, visit their website directly to find out.