TrustLayer™

QR code attacks

There are two main types of QR code attacks to watch out for:

Quishing

Quishing attacks take place when a cybercriminal sends a phishing email containing a malicious QR code attachment.

The email text will encourage the victim to scan a QR code and once this is done, it can either install malicious software on the device or direct the victim to a phishing page which captures sensitive data.

QRL jacking

Most organisations will use a QRL – or quick response login – as an alternative to the standard password. This allows you to login to your accounts by scanning a QR code through your authentication app.

QRL Jacking attacks work by replacing the legitimate QRL with a malicious one, which once scanned, compromises the device and gives the attacker access.

How can you prevent these types of attacks?

01 If you believe the QR code has not come from a reliable source, or you are unfamiliar with the sender, avoid scanning it

02 If the QR code is being used as a request for payment or any other sensitive data, contact the source through another method to check this is legitimate

03 If you encounter a QR code in public, be sceptical and never just scan one to see where it might lead

04 Use a QR code scanning app, rather than just your camera. These apps are more likely to offer a preview of the URL before you open it, so you can check whether the website looks secure and legitimate before you visit