The Threat of QR Code Scams

The adoption and use of QR codes has grown massively in the last 5 years.

Three factors have contributed to this;- the increase in global smartphone penetration, better access to high-speed mobile internet and how convenient they are to use.

Globally, in 2022, 4% of all consumer payment transactions were via QR Codes, according to a survey by Kleiner Perkins Caufield & Byers, Visa Inc., and GfK.

Cybercriminals love popular technologies and focus on them to scam, hack, cause malware infection, and more. This massive adoption of the technology has subsequently led to a rise in scams revolving around scanning QR codes.

As a reminder and follow up to my previous articles on various types of internet-based financial scams, including PayPal and The War on Investment Fraud, here is a quick review of how these delightful people use QR codes to try to scam you, stealing personal details and money.

Types of QR Code Phishing Scams

QR codes work by embedding instructions into a black and white dot-based image. They work a little like the barcodes you see on food packaging in a supermarket.

A smartphone camera, app, or QR code scanning device scans the QR code. The scan then translates the data into human-readable information. QR codes usually contain web links or links to media such as videos or links to download an app. This use of links in a QR code provides a cybercriminal with the opportunity to go phishing.

There are a few variations on the QR code scam theme doing the rounds:

1. Quishing (QR-Phishing)

Quishing is a mashup of QR codes and email phishing where the fraudsters embed a malicious QR code into a legitimate-looking email.

A recent example of a quishing attack was a Microsoft Office 365 phishing campaign that used QR codes to steal log-in credentials. Researchers identified spoof Office 365 emails that offered access to missed voicemail messages by scanning a QR code.

Scanning the QR code took the user to a fake Office 365 page, which requested credentials to gain access to the message.

QR codes are also being used in various regular scam types, such as tax scams.

The UK government department responsible for the collection of taxes, the HMRC, recently added support for QR codes on their website. However, fraudsters have now used this new feature as a basis for a new QR code tax phishing scam.

A spoof HMRC email asks the recipient to scan the code to pay overdue tax. The QR code takes the taxpayer to a spoof site where their financial information is then stolen.

2. QRL Jacking (Quick Response Code Login)

This is an older version of the more recent Quishing scam, but one that has phishing implications.

QR codes are very convenient for users, and some companies have extended this convenience to their log-in systems, where users scan a QR code to log into an account.

In QRL Jacking, an attacker navigates to a legitimate site, initiating a session and generating the QR code to log in. The attackers then capture this QR code (for example, using screen scraping) and places this legitimate QR code on a spoof site.

The attacker then uses spear-phishing to target an individual, tricking them into going to the spoof site. The person targeted will then use the captured QR code to log-in; this logs into the original session, thus logging the attacker into the legitimate account.

This scam is more challenging to carry out as it is time-sensitive; however, it will be worth the effort if this is a high-value or sensitive account.

3. QR Crypto-quishing (QR Code cryptocurrency scams)

QR codes are often used to make it more convenient to download a legitimate app. However, they can be used to encourage people to download malicious apps, including crypto-wallets.

For example, the QR crypto-quishing scam involves capturing persistent consent (prior authorisation) to use the wallet; this allows the fraudster to drain the wallets of cryptocurrency.

4. Drive-by QR Code Phishing

Drive-by-downloads of malware are one of the most insidious forms of malware infection.

A person must land on an infected site, and a flaw in any software they use can open the door to malware infection.

QR code phishers take advantage of drive-by-download opportunities by sending phishing emails with QR codes that take the recipient to an infected website.

One scan of the code and their mobile device may become infected with a trojan.

Tips to avoid QR code scams

Here are some tips to spot and avoid fraudulent QR code scams:

Most importantly, **slow down** - A QR code is a tool that encourages you to act quickly and that's what the fraudsters want you to do – Act quickly, and without thinking.

QR stands for "quick response." It works well for advertisers, but it's important to take your time and assess if you need to scan the code, and whether the information being asked for is legitimate.

Once you've scanned the QR code, check the domain address that appears at the top of the browser. A red flag that the website or app that you've been directed to is a scam is when the domain doesn't match the organisation that provided the code. Close your browser page if the QR code you scanned opens up a suspicious site.

Avoid scanning a QR code if it looks like a sticker covering another QR code.

For example, an advertisement on the street. Scammers can print fraudulent codes on stickers and affix them to legitimate ads.

If you're unsure about the legitimacy of the QR code, just manually search for the website you need.

If you think you've been scammed

Banks and other financial institutions take extensive steps to protect your personal information entrusted to them and to help you protect it as well. If you think you've been the victim of a QR code scam and provided your financial information to a fraudster, contact your bank immediately.