QR - QUICK RESPONSE CODE

QR CODE?

QR code - quick response code is a type of invented in 1994 by the Japanese automotive company. In practice, QR codes often contain data for a locator, identifier, or tracker that points to a website or application.

The Quick Response system became popular outside the automotive industry due to its fast readability and greater storage capacity. Applications include product tracking, item identification, time tracking, document management, and general marketing.

QR code consists of black squares arranged in a square grid on a white background, which can be read by an imaging device such as a camera.

QR code is a square barcode that a smartphone camera can scan and read to provide quick access to a website, to prompt the download of an application, and to direct payment to an intended recipient.

QR CODE FRAUDS

The most common type of QR code fraud operates like a phishing scheme. Fraudsters create a fraudulent QR code, or manipulate a legitimate QR code, to direct consumers to a malicious website that will steal their money or information. These fraudulent QR codes might be encountered online, in emails, text messages or anywhere in the physical world.

In the digital space, QR code fraud often begins with an email, text message or social media post that uses social engineering techniques to convince the user to scan the code. The message may claim to be from a trusted company or financial institution. Users who scan the code are directed to a malicious website that looks legitimate but is designed to steal their money or information.

In another type of scheme, fraudsters use QR codes to expose the user's device to malware. The QR code might direct the user to a malicious website that downloads the malware onto their device, or the malware might be embedded in the QR code itself. Once the malware has infected the device, fraudsters can steal the user's information.

- Cybercriminals tamper with both digital and physical QR codes to replace legitimate codes with malicious codes. A victim scans what they think to be a legitimate code but the tampered code directs victims to a malicious site, which prompts them to enter login and financial information. Access to this victim information gives the cybercriminal the ability to potentially steal funds through victim accounts.
- Malicious QR codes may also contain embedded malware, allowing a criminal to gain access to the victim's mobile device and steal the victim's location as well as personal and financial information. The cybercriminal can leverage the stolen financial information to withdraw funds from victim accounts.
- Businesses and individuals also use QR codes to facilitate payment. A business provides customers with a QR code directing them to a site where they can complete a payment transaction. However, a cybercriminal can replace the intended code with a tampered QR code and redirect the sender's payment for cybercriminal use.

PROTECT YOUR SELF

Once you scan a QR code, check the URL to make sure it is the intended site and looks authentic. A malicious domain name may be similar to the intended URL but with typos or a misplaced letter.

Practice caution when entering login, personal, or financial information from a site navigated to from a QR code.

If scanning a physical QR code, ensure the code has not been tampered with, such as with a sticker placed on top of the original code.

Do not download an app from a QR code. Use your phone's app store for a safer download.

If you receive an email stating a payment failed from a company you recently made a purchase with and the company states you can only complete the payment through a QR code, call the company to verify. Locate the company's phone number through a trusted site rather than a number provided in the email.

Do not download a QR code scanner app. This increases your risk of downloading malware onto your device. Most phones have a built-in scanner through the camera app.

If you receive a QR code that you believe to be from someone you know, reach out to them through a known number or address to verify that the code is from them.

Avoid making payments through a site navigated to from a QR code. Instead, manually enter a known and trusted URL to complete the payment.

References:

https://en.wikipedia.org/wiki/QR_code (WIKIPEDIA)

https://www.ic3.gov/Media/Y2022/PSA220118 (FBI)

https://www.ic3.gov/Media/Y2022/PSA220118 (ACFE)