(Approx. 1177 words)

QR Code Scams – Be careful where you point that smartphone

By Phil Sorrentino, Secretary and APCUG Rep, Sun City Center Computer Club

<https://scccomputerclub.org/>

philsorr (at) yahoo.com

QR Codes seem to be everywhere today. You'll find them anywhere someone wants to give you more information than is possible by other means, like a sheet of paper or a machine-readable standard bar code. Initially, QR codes were created to track manufacturing processes where barcodes couldn't store enough information. However, a bar code has one dimension. A QR code is 2-dimensional and can store significantly more data than a bar code. Roughly speaking, a QR code may contain as many as 7,000 characters as opposed to a bar code that may contain up to around 40 characters. That's over 170 times the amount of data. This increased amount of information makes the QR code so worthwhile.

QR codes were invented in Japan in the 1990s. They were first used by the automotive industry to manage production but have spread everywhere. There are even websites and apps that let you make your own.  A QR code is a machine-readable, 2 dimension matrix of black and white squares. A QR code may represent many different data types, such as text, a hyperlink to a website, a telephone number, an email address, or a text or email message. QR codes, like billboards, clothing labels, walls, TVs, and even tattoos, can be placed on almost anything. QR stands for Quick Response. Quick Response comes from the manufacturing industry and deals with how fast a product can be replaced on the seller's shelves. Quick Response is "the rapid replenishment of a customer's stock by a supplier with direct access to data from the customer's point of sale." A QR code is merely a data storage representation of some information using the binary code. (For example, the letter A is represented by "01000001") The little squares and patterns of the QR code represent the binary information. The actual QR code is read-only, so it cannot record or steal any personal information on its own. Nowadays, the smartphone's camera app can scan the QR code when the camera is directed at it. (Most smartphones no longer have to download a separate app from the App store for reading QR codes.)

A QR code with an embedded hyperlink to a website can connect you to a specific website quickly and easily using your smartphone. There is very little one needs to know to take advantage of a QR code. But a lot of the latest technology is being used to accomplish the task. The three major technology components are your smartphone, the internet, and a server (on the internet, or "in the cloud"). This collection of technologies goes by the name "Client-Server Technology," and all three components have been developed to work together. For example, your smartphone has a camera App that connects the smartphone, as the client, to the server website whose URL was embedded in the QR code. (URL is the Universal Resource Locator, the term for a web address on the internet.) This allows the provider of the QR code the ability to connect your phone with the QR code provider's server when you scan the QR code. Once connected to the server, the smartphone can access all the information that the server can provide.

QR codes take people from the physical world to the online (cyber) world. They let smartphones connect to an enormous world of information quickly and easily, but unfortunately, they also allow smartphones to connect quickly and easily to a scammer's website. This is why scammers have started using QR codes in attempting to get in touch with potential victims. It gets people online with the scammer's server. It is similar to "phishing" emails and telephone calls. QR codes are another way for scammers to get in touch with potential victims.



Many scammers (aka cybercriminals) have started to exploit the technology's convenience. Scammers create malicious QR codes to connect unwitting consumers to the scammer's server and dupe them into divulging their personal information. Anytime new technology comes out, cybercriminals attempt to find a way to exploit it. This is especially true with technology like QR codes. It seems like most people can figure out how to use them, but they probably don't really know how they work, and it's always easier to manipulate people when they don't understand their technology. Scanning the scammer's QR codes won't do anything malicious to your smartphone, such as installing malware. Still, it probably will take you to a website designed to try to get personal or financial information from you.

Like any other phishing scheme, it's impossible to know precisely how often QR codes are used for malicious purposes. Experts say they still represent a small percentage of overall phishing, but numerous QR code scams have been reported to the Better Business Bureau. As a result, many people know they need to be on the lookout for phishing links and questionable attachments in emails that purport to be from your bank. But thinking twice about scanning a QR code with your smartphone camera isn't second nature for most people yet.

Recently a QR code scam was uncovered in a Texas city. Drivers were led to a scammer's website after scanning a QR code sticker on a parking meter. Eventually, around 30 such stickers were found. The QR code was supposed to help the motorist pay for online parking. However, instead of being taken to the city's authorized website, the motorist who scanned the fake stickers was led to a fake website that collected their credit card information. With a warning of the parking meter scam, officials in another city issued a warning to motorists after spotting similar stickers on parking meters.

Fake QR codes have even shown up in emails. Scammers may like using QR codes in phishing emails because they often aren't picked up by security software, giving them a better chance than attachments or bad links to reach their intended targets. It boils down to QR codes being just one more way for cybercriminals to get what they want and yet another threat for people to be on the lookout for.

**So be careful when scanning QR codes. Here are some tips from security experts. Think before you scan. Be especially w**ary of codes posted in public places. Take a good look and determine if the sticker is part of the sign or display. If the code doesn't look like it fits in with the background, it may have been put there by a scammer. Be suspicious of any QR code that comes in an email. If you scan a QR code, look at the website it led you to and determine if it looks like what you expected. If it doesn't look appropriate, then leave the website. If it asks for personal information you don't think is appropriate, don't provide it. And, in the words of one of the Computer Club's past presidents, Matt Batt, "Be careful out there!"