How QR codes work, and what makes them dangerous: A computer scientist explains

April 8 2022, by Scott Ruoti

The QR code anatomy: data (1), position markers (2), quiet zone (3) and optional logos (4). Credit: Scott Ruoti, CC BY-ND

Among the many changes brought about by the pandemic is the widespread use of QR codes, graphical representations of digital data that can be printed and later scanned by a smartphone or other device.

QR codes have a wide range of uses that help people avoid contact with objects and close interactions with other people, including for sharing restaurant menus, email list sign-ups, car and home sales information, and checking in and out of medical and professional appointments.

QR codes are a close cousin of the bar codes on product packaging that cashiers scan with infrared scanners to let the checkout computer know what products are being purchased.

Bar codes store information along one axis, horizontally. QR codes store information in both vertical and horizontal axes, which allows them to hold significantly more data. That extra amount of data is what makes QR codes so versatile.

Anatomy of a QR code

While it is easy for people to read Arabic numerals, it is hard for a computer. Bar codes encode alphanumeric data as a series of black and white lines of various widths. At the store, bar codes record the set of numbers that specify a product's ID. Critically, data stored in bar codes is redundant. Even if part of the bar code is destroyed or obscured, it is still possible for a device to read the product ID.

QR codes are designed to be scanned using a camera, such as those found on your smartphone. QR code scanning is built into many camera apps for Android and iOS. QR codes are most often used to store web links; however, they can store arbitrary data, such as text or images.

When you scan a QR code, the QR reader in your phone's camera deciphers the code, and the resulting information triggers an action on your phone. If the QR code holds a URL, your phone will present you with the URL. Tap it, and your phone's default browser will open the webpage.

QR codes are composed of several parts: data, position markers, quiet zone and optional logos.

The data in a QR code is a series of dots in a square grid. Each dot represents a one and each blank a zero in binary code, and the patterns encode sets of numbers, letters or both, including URLs. At its smallest this grid is 21 rows by 21 columns, and at its largest it is 177 rows by 177 columns. In most cases, QR codes use black squares on a white background, making the dots easy to distinguish. However, this is not a strict requirement, and QR codes can use any color or shape for the dots and background.

Position markers are squares placed in a QR code's top-left, top-right, and bottom-left corners. These markers let a smartphone camera or other device orient the QR code when scanning it. QR codes are surrounded by blank space, the quiet zone, to help the computer determine where the QR code begins and ends. QR codes can include an optional logo in the middle.

Like barcodes, QR codes are designed with data redundancy. Even if as much as 30% of the QR code is destroyed or difficult to read, the data can still be recovered. In fact, logos are not actually part of the QR code; they cover up some of the QR code's data. However, due to the QR code's redundancy, the data represented by these missing dots can be recovered by looking at the remaining visible dots.

Are QR codes dangerous?

QR codes are not inherently dangerous. They are simply a way to store data. However, just as it can be hazardous to click links in emails, visiting URLs stored in QR codes can also be risky in several ways.

The QR code's URL can take you to a phishing website that tries to trick

you into entering your username or password for another website. The URL could take you to a legitimate website and trick that website into doing something harmful, such as giving an attacker access to your account. While such an attack requires a flaw in the website you are visiting, such vulnerabilities are common on the internet. The URL can take you to a malicious website that tricks another website you are logged into on the same device to take an unauthorized action.

A malicious URL could open an application on your device and cause it to take some action. Maybe you've seen this behavior when you clicked a Zoom link, and the Zoom application opened and automatically joined a meeting. While such behavior is ordinarily benign, an attacker could use this to trick some apps into revealing your data.

It is critical that when you open a link in a QR code, you ensure that the URL is safe and comes from a trusted source. Just because the QR code has a logo you recognize doesn't mean you should click on the URL it contains.

There is also a slight chance that the app used to scan the QR code could contain a vulnerability that allows malicious QR codes to take over your device. This attack would succeed by just scanning the QR code, even if you don't click the link stored in it. To avoid this threat, you should use trusted apps provided by the device manufacturer to scan QR codes and avoid downloading custom QR code apps.

Provided by The Conversation

Citation: How QR codes work, and what makes them dangerous: A computer scientist explains