# QR Code Dangers and The Risks Behind Using Them

There's danger now lurking behind those busy black-and-white boxes that are QR codes and that now seem to be found everywhere for everything, including viewing restaurant menus. Always a quick way to scan for information, businesses are using them now more than ever. A study by the Ivanti Research Group takes a look at what's really going on behind QR's and their findings should make anyone think twice before they reach to scan a QR code with their mobile device.

QR codes started popping-up in 1994 for help with automobile manufacturing in Japan, but they've come a long way since then. The letters QR stand for "quick response" and Ivanti found 57% of survey respondents increased QR code scanning since mid-March last year. During the height of the pandemic, they provided a quick and safe way to get information for everything from restaurant menus, to doctor appointments and prescriptions. But thanks to hackers, the word "safe" no longer applies to QR codes.


## Are you a Good QR or a Bad QR?

As harmless as those busy little black-and-white boxes look, cybercriminals are often behind them. Ivanti found 87% of QR users feel safe using them for financial transactions. However, they also found 31% of users say that after scanning a QR code, they were brought to a suspicious website or experienced something they were not expecting.

Hackers are using QR's to redirect users to websites that look legitimate, but in reality, can steal credit card data and login credentials. Still others are brought to sites that automatically download malicious software onto the mobile device, compromising all accounts, apps and data they hold with no action required from the user. Unfortunately, the lack of security software on mobile devices helps facilitate these crimes.

The most common type of QRLjacking (Quick Response Code Login Jacking) is when a legitimate QR code used for cashless payments is replaced with malicious QR code that enables a hacker  to transfer money out of financial accounts.

## Four QR Attack Methods:

1. **First**, criminals can inject your phone with malware. This direct approach requires nothing more than an unsuspecting consumer or employee to scan a QR code out of curiosity leading to an infected website. Just visiting the infected website can trigger a malicious download. One example of how they might deliver this attack method is to send the QR code in an email that appears to be legitimate, enticing the user to scan it.
2. **Second**, the attacker leads you to a phishing site to steal your credentials or to gain access to your private information on your mobile device. Phishing websites can be very hard to detect. They use a similar-looking Universal Resource Locator (URL) to a trusted website. Another approach is to change the domain extension. For example, they change the '.org' to '.com'. Other times, there is a slight change in the spelling of the URL so hard to distinguish that it tricks the user. Once the user visits the phishing site, username/login credentials are requested. After the attacker has your login, the rest is history. They can access your accounts, make changes, see private information and cause irreversible damage to your financial health.
3. **Third**, cybercriminals can print out free encoding tools on the internet to make QR codes. They print the QR code on adhesive paper and place it over a legitimate QR code, or they can email a malicious QR code to an unexpecting consumer.
4. **Fourth**, there's always the risk that an attacker finds a bug in a code reader application that could result in the exploitation of cameras and/or sensors in phones or other devices.

The truth is many of us are curious individuals and may be tempted to scan a QR code just to see what it is. People wonder if it will bring them to a website, a coupon, or a code for free products. Many do not take the time to consider that fact that this action might have huge consequences, such as injecting malware on either their company owned or personal devices.

## Four Security Measures:

1. **First**, never scan a QR code from an untrusted source, whether it be in an email or a physical place.
2. **Second**, when possible, feel the QR code to see if a sticker has been applied over the original and legitimate QR code.
3. **Third**, only use a QR reader application with built-in security features. Understand that some QR reader apps are more secure than others. Important features to look for include showing the content of the link before it is visited and checking the link against a database of known malicious links.
4. **Fourth**, if you find a malicious QR code, report it to the owner of the business where you discovered it.

New technology brings new vulnerabilities, creating a need for ongoing awareness and cybersecurity education. The key is to do what you should do when faced with risk: Take precautions!