

A Quick Look at QR Codes

When QR scanning breaks security

You've seen them everywhere: in ads, on restaurant menus, even on business cards and concert flyers. It's the little black-and-white square that says "Scan here!" It's a QR code, or Quick Response code.

Think of a QR code like a bar code at the grocery store. The code contains information, such as a website URL. When your phone reads the code, it essentially reads an instruction to access that website.

But it's an instruction that you yourself can't read. This means that a QR code could be telling your device anything, and you won't know until it's too late.



In one case, hackers targeting a US energy company sent employees documents containing QR codes. The messages stated that the person should scan the QR code to update their employee account information.

This led them to a phony website where they entered their information, which the hacker promptly stole.

Why did it work? The QR code obscured the link, making it difficult for the victim to recognize where they were being sent. Embedding the QR code in a document or PDF also helped the malicious link bypass the company's security filters.

In another case, scammers used QR code stickers on parking meters to direct drivers to a phony payment system. Imagine thinking you've paid for parking and getting towed anyway!

Remember: you don't know what a QR code does until you scan it. If you aren't absolutely certain that code is safe, then QR should stand for **"Quit Responding."**

From redirection to authorization

QR codes can do more than just send you to a phony website. Some malicious QR codes contain instructions for the device to authorize a dangerous action. In one common example, the QR code instructs the device to allow access by a hacker-controlled application. Now the hacker has a back door into your personal device.

