Published on *University of Colorado* (https://www.cu.edu)

What is Quishing and How to Protect Yourself [1]

Quishing is the use of a QR code that directs you to a fraudulent website. Once on the site, cybercriminals work to steal your personal and financial information. The design of QR codes makes it impossible for the user to know where the code will direct them after scanning.

“The QR codes are very real. It's the destination that may cause the problem, which is why I think QR codes are dangerous right now,” said Charles Wertz, Information Security Officer for UCCS. “Generally, these codes work, but a cybercriminal's intent is to have an unsuspecting person scan the code and be taken to a fraudulent website.”

Common scams include a fake parking ticket placed on your car windshield that contains a QR code to pay the fine, or a QR code placed on the back of a parking meter, leading you to assume that it’s a method for payment.

Tips From the FBI to Avoid Becoming a Victim

- Once you scan a QR code, check the URL to make sure it is the intended site and looks authentic.
- 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.
- Avoid making payments through a site navigated to from a QR code. Instead, manually enter a known and trusted URL to complete the payment.
- 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.
- Do not download an app from a QR code. Use your phone’s app store for a safer download.
- If you receive an email from a company, you recently made a purchase with stating a payment failed 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.
- 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.

Groups audience:
Office of Information Security

Links
[1] https://www.cu.edu/security/what-quishing-and-how-protect-yourself