# QR codes: Is it safe to scan?

February 17 2022, by Kim McGrath

Credit: Pixabay/CC0 Public Domain

The Coinbase Super Bowl commercial that featured a bouncing QR code set to music was so popular it caused the cryptocurrency app to temporarily crash. What does this tell us about how these codes are being used and how safe it is to scan? Wake Forest Computer Science Professor Sarra Alqahtani answers questions about QR codes, cybercrime and how to keep your personal information safe.

## As a computer science professor studying

## cybersecurity, what was your reaction to the Coinbase commercial?

It was a fun commercial to watch, but I immediately started thinking about how normalized this technology becomes without an equivalent awareness about its security issues. As with any new technology, security comes usually as an afterthought not only for the developers but for the users as well. I'm hoping for an effort to educate people about QR code security concerns and how to protect their privacy.

## How likely is it that private information can be compromised by scanning a QR code?

The QR code can be replaced by a malicious one (the simplest way is by physically pasting one code on top of another), which could lead the user to a fake website that is similar looking to the original website. The hacker then can plant a small software (malware) in the user's phone to track and collect their data.

## What do hackers do with the information they steal?

They can steal the usernames and passwords we use in different apps and websites and sell them on the dark web. This data can be used to guess user/employee credentials during other attacks—like what happened in the Colonial Pipeline ransomware attack.

## Is there a way to know if a QR code is safe?

We can't recognize any difference between the legitimate and malicious codes with our eyes but when we scan the code we should pay attention to the website link before clicking on it. That's why it is recommended to include the website link with the code when sharing it publically.

## What should we look for when checking a URL before clicking?

If there is a security risk, the URL will look similar to the original URL but with slight changes. For example, instead of www.yahoo.com, the hacker may use yaho0.com which looks very similar. This kind of trick falls under the field of phishing attacks which has a long history in cybersecurity.

## What is your best advice for protecting personal information when using QR codes?

I recommend not scanning the QR codes as much as possible and using paper manuals and menus. I also advise using the built-in cameras in smartphones instead of using third-party apps since the built-in cameras show the website link and ask the user to click on it, which is not usually the case with third-party apps.

## If you suspect you have clicked on a fake website and malware has been installed, what should you do?

It depends on the phone you are using but in general, you should clear your browser cache, back up your files, change your credentials. If your phone doesn't have built-in protection you will need to use malware detection software to detect and remove any malware.

## Do you have a book or resource you could recommend for those who want to know more about QR codes?

Read the FBI's Public Service Announcement, "Cybercriminals Tampering with QR Codes to Steal Victim Funds."

**More information:** FBI announcement: www.ic3.gov/Media/Y2022/PSA220118

Provided by Wake Forest University

Citation: QR codes: Is it safe to scan? (2022, February 17) retrieved 5 May 2024 from https://techxplore.com/news/2022-02-qr-codes-safe-scan.html