Cybersecurity trends are heating up

QR code dangers[1]

Quick Response (QR) codes are seen everywhere these days. They have replaced restaurant menus, used in TV commercials, and even spotted on the side of city buses. There is no doubt that QR codes are convenient for accessing information, but it is not always the safest thing to use.

Hackers can easily use QR codes to gain access to our devices. They will simply place their QR codes around public areas, waiting to see who will scan them. They might create a fake advertisement or attach it to a legitimate ad.

The most significant danger of QR codes is the lack of transparency about where the code will take you. People are quick to scan these codes without hesitation because they have become standard practice for many businesses, and hackers have come to exploit them. We might not think of it, but a malicious website could be hidden behind the link. The code could deliver malware to your phone, collecting your personal information, passwords, and account information.

QR code safety

The easiest way to stay safe against a malicious website hidden behind a QR code is to simply not scan it.

Go straight to the source. The official website is often listed along with the QR code, so type that in instead of using the scannable code. It might not save you time, but it could save your information.

If you do choose to scan a QR code, look for the pop-up that shows the website URL. Check carefully to see if it looks authentic. A malicious URL might look very similar to the website you are trying to go to but will have misplaced letters or typos.

Do not download a QR code scanning app. The app could increase your chances of downloading malware. Just use your phone camera, as many phones already have this embedded.

If you receive a physical code to scan, check to ensure that it hasn't been tampered with. Sometimes hackers will place a sticker on top with a new code.

China is under fire with the world's largest data breach[2]

Records stolen from police in Shanghai contain data on one billion Chinese citizens. According to experts, the database might have been misconfigured and exposed by human error back in 2021 when a technical blog post was published on a Chinese developer website in 2020. This meant anyone that could access the database without a password if they knew the web address. "Security researchers frequently scan the internet for exposed databases or other sensitive data...but threat actors also run the same scans." In this case, the hacker found the information, gathered it, and deleted it, leaving a ransom note "demanding ten bitcoins for its return."

The news of this breach is not widely reported in China, where their speech and internet access are under tight restrictions. For more information on this breach, visit: https://techcrunch.com/2022/07/07/china-leak-police-database/

1 https://www.ic3.gov/Media/Y2022/PSA220118 FBI PSA "Cybercriminals Tampering with QR Codes to Steal Victim Funds" 2 https://techcrunch.com/2022/07/07/china-leak-police-database/