Lancashire
Cyber Foundry

QR Codes:

Convinience vs. Security Risks

READ TIME: 2 MINS

AUDIENCE: BUSINESS & TECHNOLOGY

QR codes, or Quick Response codes, have become ever-present in our daily lives as they make for a rapid and effective method of transmitting information, be it banking systems or menus at restaurants.

According to anti-phishing software TitanHQ, over 34% of smartphone users scan a QR code once a week and nearly 84% have scanned a QR code at least once.

Due to this popularity, "QR code phishing" has become more prevalent, giving hackers more opportunities to extort, hack, and infect computers with malware. This article discusses the possible risks posed by QR codes and demonstrates how to mitigate them.

WHAT ARE QR CODES

QR codes are two-dimensional barcodes that can be scanned using a smartphone camera or a specialized QR code reader. These codes are used to quickly and efficiently convey information such as website URLs, payment information, and contact information.

QR CODES AND CYBER

Cybercriminals now frequently use QR codes to spread malware, conduct phishing scams, and steal confidential data.

Using fraudulent QR codes is one of the most widely used strategies. These harmful codes are created to mimic authentic ones, but when they are scanned, they direct viewers to a bogus website. These fake websites may prompt users to enter their personal information, such as credit card numbers or login credentials, which can then be used for fraudulent purposes.

Injecting code into QR codes is another method for taking advantage of them. A QR code's source code can be altered by attackers, who can then insert malicious instructions that can control the user's device or even steal important data. For instance, they can produce a QR code that links to a webpage with malware that, when accessed, infects the user's device.

European Union
European Regional
Development Fund

NORTHERN POWERHOUSE HM Government

Lancaster University

Moreover, it's possible that users may then be directed to phishing websites that demand they download dangerous apps. And if downloaded, these apps can gain access to the infected device, track activities, and breach data. Hackers may also use QR codes to circulate ransomware, which may go as drastic as preventing individuals from using their devices unless they pay a ransom.

PROTECTING YOURSELF

There are several steps you can take to protect yourself from QR code scams:

- Only scan QR codes from trusted sources. If you are unsure of the source of a QR code, do not scan it.

- Use a trusted QR code reader. Be sure to download a QR code reader from a trusted source, such as the App Store or Google Play.

- Check the URL before entering payment information. Before entering payment information on a payment page, check the URL to ensure that it is legitimate. Attackers may use a slightly different URL to trick users into entering their payment information.

- Be wary of unsolicited QR codes. If you receive a QR code via email or text message from an unknown sender, do not scan it.

- Keep your device up to date. Make sure your device is running the latest version of its operating system and that all security patches have been installed. This can help protect your device from malware infections.

CONCLUSION

In conclusion, while QR codes may seem like a harmless convenience, they can pose a significant risk to cyber security if used improperly. It is important for users to be aware of the potential dangers and take steps to protect themselves, such as scanning codes only from trusted sources, using secure QR code scanners, and keeping their devices up to date with the latest security updates. By following these guidelines, users can enjoy the convenience of QR codes while avoiding the potential risks associated with them.

ABOUT THE AUTHOR

Anjana Shukla

I am a MSc Cyber Security Student at Lancaster University. Before coming here, I have worked for 2 IT companies namely Infosys Ltd. and Mindtree Ltd. as Systems Engineer and Senior software engineer.

I gained quite varied understanding of how this industry works and how much loss an organization can face with only a single technical breach. And ever since, I have only gotten more curious about cyber security.