Cyber Crime Information - 153

April 26th, 2022

Subject: Cybercriminals Tampering with QR Codes to defraud Citizens

Threat Summary

Cybercriminals are tampering with Quick Response (QR) codes to redirect victims to malicious sites that steal login and financial information.

A QR code is a square barcode that a smartphone camera can scan and read to provide quick access to a website, to prompt the download of an application, and to direct payment to an intended recipient. Businesses use QR codes legitimately to provide convenient contactless access and have used them more frequently during the COVID-19 pandemic. However, cybercriminals are taking advantage of this technology by directing QR code scans to malicious sites to steal victim data, embedding malware to gain access to the victim's device, and redirecting payment for cybercriminal use.

Fig. 01 – Tampered QR Codes used for cyber frauds

Modus Operandi

- Cybercriminals tamper with both digital and physical QR codes to replace legitimate codes with malicious codes.
- When victims scan what they think to be a legitimate QR code but the tampered code directs victims to a malicious site, which prompts them to enter login and financial information.
- Malicious QR codes may also contain embedded malware, allowing a criminal to gain access to the victim's mobile device and steal the victim's location as well as personal and financial information.
- The cybercriminals leverage the stolen financial information to withdraw funds from victims' accounts or deceive victims into making fraudulent payments.

Suggestions

- After scanning 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 on a site opened using a QR code.
- Ensure the QR code has not been tampered with, such as with a sticker placed on top of the original physical QR code.
- Avoid downloading an app from a QR code. Use your phone's app store for a safer download.
- Verify with the company (through contacts on official websites) if payment for an article/service is requested via QR Code.
- Verify by calling a known number (of sender) that the sent QR code payment link is authentic.
- Avoid making payments through a site navigated to from a QR code. Instead, manually enter a known and trusted URL to complete the payment.
- Report any such incidents on the ***cybercrime.gov.in*** portal and follow ***@CyberDost*** on Twitter, YouTube, Facebook, Instagram, Public, Koo and LinkedIn to know more about safety tips.

Regards,

Indian Cyber Crime Coordination Centre
CIS Division, MHA
011-23438207