January 18, 2022
Alert Number
I-011822-PSA
Questions regarding this PSA should be directed to your local **FBI Field Office**.

Cybercriminals Tampering with QR Codes to Steal Victim Funds

The FBI is issuing this announcement to raise awareness of malicious Quick Response (QR) codes. Cybercriminals are tampering with 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.

Cybercriminals tamper with both digital and physical QR codes to replace legitimate codes with malicious codes. A victim scans what they think to be a legitimate code but the tampered code directs victims to a malicious site, which prompts them to enter login and financial information. Access to this victim information gives the cybercriminal the ability to potentially steal funds through victim accounts.

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 cybercriminal can leverage the stolen financial information to withdraw funds from victim accounts.

Businesses and individuals also use QR codes to facilitate payment. A business provides customers with a QR code directing them to a site where they can complete a payment transaction. However, a cybercriminal can replace the intended code with a tampered QR code and redirect the sender's payment for cybercriminal use.

While QR codes are not malicious in nature, it is important to practice caution when entering financial information as well as providing payment through a site navigated to through a QR code. Law enforcement cannot guarantee the recovery of lost funds after transfer.

TIPS TO PROTECT YOURSELF:

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

If you believe you have been a victim of stolen funds from a tampered QR code, report the fraud to your local FBI field office at www.fbi.gov/contact-us/field-offices. The FBI also encourages victims to report fraudulent or suspicious activities to the FBI Internet Crime Complaint Center at www.ic3.gov.