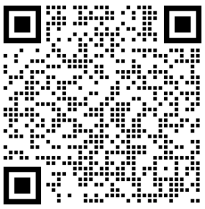
Cybercrime Prevention Flyer

CPF 00003-2021-CID361-9H 1 March 2021

QR Code Fraud



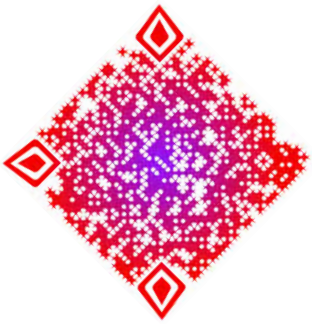
Quick response codes, known as QR codes, were originally developed in the mid-1990s for manufacturing and inventory control. Not to be mistaken with the Universal Product Code, often referred to as a UPC code or barcode, found on most products in U.S. stores, QR codes can be seen in many places and used for many reasons.

Most often, a QR code looks like randomly placed small black squares arranged in a borderless square. QR Codes can, however, be quite customized with different colors and different backgrounds.

In these days of COVID-19, where touch-free interactions are encouraged, people are seeing QR codes used more frequently and in new ways, such as in restaurants. Where once a paper menu, wine list, or drinks menu was handed to a diner, now a QR code, printed on a single-use paper, is presented. Sometimes a QR code, printed on an adhesive label, is affixed directly to a stationary surface.

Regardless of how the QR code is deployed, the patron need only frame it in a smart phone camera to read it. Although there are QR specific applications for reading QR codes, the cameras on up-to-date smart phones read QR codes natively and open documents.

Easy, effective, fast, economical, and touch free. All of these are qualities wanted in the days of COVID-19.



But, like just about everything good in computers or on the internet, if it can be used for good, it can and will be used for bad. The same is true of QR codes. Someone with bad intentions can misuse QR codes. According to ThreatPost, although not rampant, QR code frauds and thefts are on the rise and developing in numerous ways.

QR codes can:

- Add nefarious contacts to the contact list.
- Connect the device to a malicious network.
- Send text messages to one or all contacts in a user's address book.
- Complete a telephone call to a telephone number that imposes charges on the calling phone.
- Send a payment to a destination where it cannot be recovered.

Report a crime to U.S. Army Criminal Investigation Command

Major Cybercrime Unit

27130 Telegraph Road
Quantico, Virginia 22134

Email

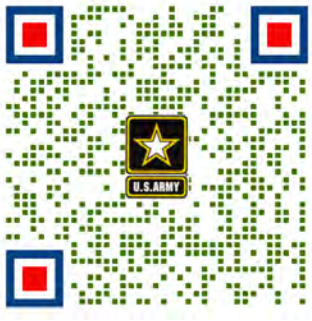
MCU Web Page

CID LOOKOUT
ON POINT FOR THE ARMY

"DO WHAT HAS TO BE DONE"

Cybercrime Prevention Flyer

A basic scam could be perpetrated by printing malicious QR codes on labels and sticking the labels to various publicly accessible surfaces. The curious passerby who scans the code is directed to a malicious website where damaging code is downloaded to their computer or smart phone.



In a more complex scam, QR codes can be used to make payments for goods and to execute money transfers. Scan the recipient's QR code. Enter the amount to transfer. Click execute. Done! Easy! Until the following day when the person making the payments discovers all of their financial accounts have been drained.

To protect yourself, many of the standard cautions apply:

- Be suspicious of unsolicited offers that seem too good to be true.
- Do not open emails from unknown senders.
- Ignore emails that ask you to provide identifying information (usernames, passwords, dates of birth, etc.).
- Do not access financial accounts by clicking links received in unexpected emails. Rather, use verified links from your bookmarks.

Specific to QR codes:

- Do not scan a randomly found QR code.
- Be suspicious if, after scanning a QR code, a password or login information is requested.
- Do not scan QR codes received in emails unless you know they are legitimate.
- Do not scan a QR code if it is printed on a label and applied atop another QR code. Ask a staff member to verify its legitimacy first. The business might simply have updated what was their original QR code.

Resources

- QR Code Security Threats – Identity Theft Resource Center
- QR Code Scam Can Clean Out Your Bank Account – Malwarebytes
- 5 Digital Payment Frauds and How to Avoid Them – The Economic Times
- Reporting Internet Crimes – Internet Crime Complaint Center
- Cybercrime Prevention Flyers – U.S. Army, Major Cybercrime Unit

To receive future MCU Cybercrime Prevention Flyers, send an email to: Subscribe CPF