UNITED STATES ARMY
CRIMINAL INVESTIGATION COMMAND

Media contact: 571-305-4041 FOR IMMEDIATE RELEASE

Army CID Cautions Rise in QR Code Scams

QUANTICO, VA (March 11, 2021) – Behavior changes this past year to reduce the spread of COVID-19 has not been lost on criminals. The Army Criminal Investigation Command's Major Cybercrime Unit is cautioning users to be wary of suspicious quick response codes, known as QR codes.

According to the Major Cybercrime Unit, QR code usage increased due to the COVID-19 pandemic. While QR codes have been around for years, COVID-19 has led to a more touch-free interaction environment and people are seeing QR codes used more frequently and in new ways, such as in restaurants. The QR code printed on a single-use paper or on a table stand is scanned with a smart phone and replaces the multiple-use paper menu, wine list, or drink menu. With a quick scan, you can pull up a restaurant menu, make a payment, or jump right to a website URL.

Originally developed in the mid-1990s for manufacturing and inventory control, QR codes are 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. However, QR Codes can be customized with different colors and different backgrounds.

Regardless of how the QR code is deployed, the patron frames it in a smart phone camera to read it. The cameras on up-to-date smart phones read QR codes natively and open documents. Making this technique fast and effective. However, cybercriminals can misuse QR codes. Although not rampant, QR code frauds and thefts are on the rise and developing in numerous ways, according to ThreatPost.com, a website about cyber security.

-MORE-

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.

The Major Cybercrime Unit warns 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 scans the code and is directed to a malicious website allowing damaging code to be downloaded to their computer or smart phone.

In a more complex scam, the QR codes can be used to make payments for goods and to execute money transfers. This tactic works when a recipient scans a QR code, enters an amount to transfer, and then executes the transaction. The following day, the person making the payments discovers all their financial accounts have been compromised.

To protect against theft, 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.

For more information about computer security, other computer-related scams, and to review previous cybercrime alert notices and cyber-crime prevention flyers visit the Army CID MCU website at https://www.cid.army.mil/mcu-advisories.html. To report a crime to Army CID, visit www.cid.army.mil.

-30-