FACT SHEET
U.S. Army Cyber Command
*The Nation's Army in Cyberspace*
www.arcyber.army.mil • www.army.mil/armycyber • @ARCYBER

## THE FACTS: QUICK RESPONSE (QR) CODES

***What are QR codes?***


Originally developed in the mid-1990s for manufacturing and inventory control, QR codes most often appear as a small graphic that looks like randomly placed small black squares arranged in a borderless square (similar to the white square in the graphic at right). But QR codes can be customized with different colors and different backgrounds. When a QR code graphic is framed in the camera of a smartphone, the code can be read by the device and immediately trigger a response, such as opening a document or a web address.

***Why are QR codes potentially hazardous?***

While QR codes make transactions fast and easy, cyber criminals and hackers can also misuse them for malicious activity or profit. According to cybersecurity experts and the Major Cybercrime Unit of the Army's Criminal Investigation Command, QR code fraud and theft are evolving and on the rise. For example, QRs that have malicious code embedded in them can be placed in publicly accessible spaces, where curious passers-by scan them, only to be directed to websites that download damaging code on their devices. The COVID-19 pandemic has also unwittingly aided the bad guys, because the codes' ability to provide a more hands-free transaction method has led to their greater use, to help prevent spread of the virus.

**What are some things malicious QR codes can do?**

Some of the nefarious things malicious codes can do include:
-- Add unwanted and potentially dangerous contacts to a contact list
-- Connect a device to a malicious network

 As of 17 March 2021

.

-- Send text messages to contacts in a user's address book
-- Make calls to telephone numbers that impose charges on the user's phone
-- Send payments to destinations where they cannot be recovered
-- Compromise financial data and accounts

***What can I do to protect myself against malicious QR codes?***

In general, CID experts recommend the same kinds of vigilance and caution you would use to protect yourself from other online hazards:
-- Be suspicious of unsolicited offers that seem too good to be true
-- Don't open emails from unknown senders
-- Ignore emails that ask you to provide identifying information such as usernames, passwords, dates of birth, etc.
-- Do not access financial accounts by clicking links received in unexpected emails; use verified links instead

And they add some cautions specific to QR codes:
-- Don't scan a randomly found QR code
-- Be suspicious if, after scanning a QR code, you are asked for a password or login information
-- Do not scan QR codes received in emails, unless you are certain they are legitimate
-- Do not scan codes printed on a label that has been applied atop another QR code, unless you can verify its validity

Source: U.S. Army Criminal Investigation Command
For more information and notices about computer security, cyber crime and computer related scams, visit the CID MCU website at https://www.cid.army.mil/mcu-advisories.html

**Follow ARCYBER on**
**(click the images to visit our pages)**

**Cyber**

ABOUT US: U.S. Army Cyber Command integrates and conducts cyberspace, electronic warfare, and information operations, ensuring decision dominance and freedom of action for friendly forces in and through the cyber domain and the information environment, while denying the same to our adversaries. As of 17 March 2021

.