FBI Warns of Scammers Using QR Codes

Article By:
Linn F. Freedman

The FBI’s Internet Crime Complaint Center (IC3) recently issued a warning alerting consumers that scammers are using malicious QR Codes to reroute unsuspecting customers to malicious sites to try to steal their data.

Also known as QRishing, criminals are taking advantage of our familiarity with QR codes after using them at restaurants and other establishments during the pandemic, to use them to commit crimes. The criminals embed malicious codes into QR codes to redirect a user to a malicious site and then attempt to get the user to provide personal information, financial information or other data that the criminals can use to perpetrate fraud or identity theft.

Embedding malicious code into a QR code is no different than embedding it into a link or attachment to a phishing email or a smishing text. Consumers are not as alert to question QR codes as we are to spot malicious emails and texts.

Hence, the alert from IC3. IC3 is warning consumers to check and re-check any URL generated by a QR code and to be cautious about using them for any form of payment.

QR codes should be viewed as suspiciously as emails and texts. Be cautious when asked to scan a QR code, and refuse to provide any type of personal information or financial information after scanning one.

Copyright © 2024 Robinson & Cole LLP. All rights reserved.