DISB
Government of the District of Columbia
Department of Insurance, Securities and Banking

GOVERNMENT OF THE DISTRICT OF COLUMBIA
MURIEL BOWSER, MAYOR

Karima M. Woods, Commissioner

DISB CONSUMER ALERT
Beware of QR Code Scams

The District of Columbia Department of Insurance, Securities and Banking (DISB) is warning residents to be on the lookout for QR (or quick response) code scams.

In the last few years, there has been a dramatic increase in the use of QR codes by businesses in an effort to help consumers instantly access smartphone applications and other electronic information. Fueled by a desire for touchless transactions during the pandemic, many restaurants stopped distributing paper menus and instead posted QR codes at tables. Diners use the QR codes to access menus, process food orders and complete payments electronically. QR codes have also proven to be convenient for tracking packages and locating information about events, recipes and healthcare tips. According to a survey by Statista, 11 million households will scan a QR code by the end of 2021.

QR CODE FRAUD

Unfortunately, QR codes can also be used for criminal purposes. Scammers can use QR codes to trick consumers into downloading malware or personal information. For example, you may receive an email, a social media message, a flyer or notice posted on a community bulletin board with a QR code promising links to useful information. Rather than take you to the application or site you intended to access, however, the QR code may take you to a phishing site that asks you to enter personally identifiable information or financial account information and credentials, all so that scammers can steal it from you. Fraudsters may even paste a phony QR code on top of an existing QR code; signs that a QR code has been tampered with is a red flag that signals a potential scam.

PROTECT YOURSELF

The Better Business Bureau suggests ways to protect yourself from becoming the victim of a QR code scam:

- Make use of QR scanner applications (apps) developed by antivirus companies to check the safety of a scanned link before you open it. The apps can identify phishing scams, forced app downloads and other dangerous links.
- Independently verify the source of the QR code, even if the source appears to be a federal, state or local government agency. Call or visit the official webpage of that agency and request that they verify the QR code's authenticity.

- Contact the sender of the QR code directly before you scan it—even if the QR code was sent to you by someone you know through the U.S. mail, an email, text or social media site—to confirm that the sender was not hacked.
- Avoid scanning QR codes presented in unsolicited emails, text messages, or social media messages arriving from someone you don't know, particularly ones that ask you to scan a QR code in order to claim a gift or take advantage of an investment opportunity.

REPORT FRAUD

If you believe you have been the victim of a QR code scam or other financial fraud, file a report with the Federal Trade Commission (FTC) at reportfraud.ftc.gov or call the FTC's Consumer Response Center at 877-382-4357. You may also contact the DISB Enforcement and Consumer Protection Division at 202-727-8000**.**

DISB Mission

Our mission is three-fold: (1) cultivate a regulatory environment that protects consumers and attracts and retains financial services firms to the District; (2) empower and educate residents and (3) support the development and expansion of business.

Follow Us on Social Media

DISB Twitter: @DCDISB
DISB Facebook: facebook.com/DISBDC

Issued: November 22, 2021