Communications Security Establishment
Centre de la sécurité des télécommunications

UNCLASSIFIED

CANADIAN CENTRE FOR
CYBER SECURITY

Security considerations for QR codes

January 2024

ITSAP.00.141

Quick response (QR) codes are small white squares with two dimensional (2D) black markings, similar in look to a barcode. QR codes contain information that can be read by your device through the camera lens. They are used in a variety of ways, like scanning to see a restaurant menu, or scanning to reach a website for additional information.

There are 3 main types of user activities related to QR codes:

- Consuming. Users scan a QR code in order to read or review something like a restaurant menu or other documents. This is the most common activity.
- Sharing. Users present their 2D code to have their information verified , like an airline boarding pass or lottery tickets. This is becoming a common practice.
- Generating. Not as common but may occur if an application requires a code to perform an action, such as pairing a smart watch to a smart phone.

QR code actions

Once scanned, the decoded text of the QR code can trigger actions such as:

- opening a website
- downloading an app
- joining a Wi-Fi network
- verifying information
- creating a contact
- sending an email or message
- dialing a phone number

Are QR codes risky?

QR codes can contain personal information. They can also execute an action, such as opening a fillable PDF or online form, that prompts you to enter personal information. Once this information has been entered, scanning the QR code will display the stored information on your device. Some online forms also create a QR code once completed.

By scanning a QR code, you could be susceptible to the following risks:

- Tracking of your online activity by websites using cookies, meaning your data can be collected and used for marketing purposes without your consent
- Collecting metadata associated to you, such as the type of device you used to scan the code, your IP address, your location and the information you enter while on the site
- Exposing financial data, such as your credit card number, if you used it to purchase goods or services on the website

The actions the QR code performs can also pose risks, such as allowing threat actors to leverage QR codes to infect devices with malware, steal personal information, or conduct phishing scams.

QR Codes as attack vectors

- **Cloning:** Threat actors clone an authentic QR code that redirects you to a malicious site or infects your device with malware to extract your personal data when you scan it.
- **Leveraging:** Threat actors use QR codes for phishing and malware attacks. Malicious QR codes can direct users to legitimate-looking websites designed to steal credentials, credit-card data, or corporate logins or to sites that automatically download malicious software onto mobile devices.
- **Advertising:** Threat actors place malicious QR codes in public areas with the hopes that people passing by will scan them.
- **Quishing:** Threat actors can use a QR code inside a phishing email, or to direct the user to a phishing website which prompts the user to disclose personal information.
- **Scanner apps:** Threat actors can use third party scanner apps to spread malware and gain access to some privacy settings on your mobile device, such as viewing your network connections or modifying the contents of your USB storage. You should use the camera built into your device or a secure code reader application to scan QR codes.

AWARENESS SERIES

Cat. No. D97-1/00-141-2023E-PDF
ISBN 978-0-660-68425-3

Reducing the risks if using QR codes

To protect your information:

- use private browsing mode on your devices and consider using a browser with anti-tracking features.
- be suspicious and carefully verify the website URL if a password or login information is requested after scanning a QR code.
- check browser settings to deactivate cookies and storage of site data.
- provide the minimum amount of personal information requested when completing online forms.
- ask for the company's privacy policy if you're scanning their code to check in or access a service.
- report suspected fraud or cyber incidents to your local police department, the Canadian Anti-Fraud Centre, or the Cyber Centre.

To protect your devices:

- configure your device to ask permission and verification before launching the QR code action.
- close your web browser if the QR code you scanned opened a suspicious site.
- turn on automatic updates for your devices.

To protect your personalized QR codes:

- keep your personalized QR codes, such as a boarding pass, in a secure folder on your device.
- allow your code to be scanned only by a secure and verified application, such as an airline or airport application.

Actions to avoid

- Authorizing your devices to automatically execute the QR code action.
- Scanning a QR code posted in a public setting, such as in a public transit station or advertisements on the street.
- Scanning a QR code printed on a label that could be covering another QR code. Ask a staff member to verify its legitimacy first. The business might simply have updated their original QR code.
- Scanning QR codes received in emails or text messages unless you know they are legitimate.
- Using QR scanner apps that are released by unknown companies or institutions.
- Putting convenience before security. Type in a website URL to view content, such as an online restaurant menu instead of scanning a QR code.

QR codes in action

In 2020, the Government of Canada supported provinces implementing QR codes as an official certificate of COVID-19 vaccines. While vaccine passports are no longer necessary in most establishments, QR codes have not lost their popularity. They are used regularly for contactless payment, on packaged food, business cards and to join Wi-Fi networks. Remember, inspection before scanning is important.

Passport applications also make use of QR codes. When applying for a passport you must to fill out a form, either electronically or by hand. Electronically completing the PDF will generate a unique QR code for your application. Be cautious when choosing this method. Even though it allows for easier data entry, it also allows anyone who scans it access to your information. Global Affairs Canada recommends that once printed, clear your computers browser cache and Adobe Acrobat viewer cache once you've printed your application to mitigate risks. Learn more about two-dimensional barcode (2D Barcode) on passport applications.

Cat. No. D97-1/00-141-2023E-PDF
ISBN 978-0-660-68425-3