Communications Security Establishment
Centre de la sécurité des télécommunications

UNCLASSIFIED

CANADIAN CENTRE FOR CYBER SECURITY

SECURITY CONSIDERATIONS FOR QR CODES

JANUARY 2022

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 became more popular and widely used during the COVID-19 pandemic, offering touchless transactions, such as replacing paper menus with a QR code that displays the online menu when scanned. QR codes have also been used for COVID-19 screenings and contact tracing. QR codes are now being used for proof of vaccination requirements which may expand the landscape for threat actors to exploit QR codes and access your personal information.

HOW DO QR CODES WORK?

QR codes contain information that can be read by your device through the camera lens. There are three main types of user activities related to QR codes:

1. Consuming is the most common activity. Users scan a QR code in order to read or review something like a restaurant menu or other documents.
2. Sharing is becoming a common practice. Users present their 2D code to have their information verified (e.g. airline boarding pass, lottery tickets, or proof of vaccination).
3. Generating is 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. 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, 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 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 they use a QR code 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

© Government of Canada
This document is the property of the Government of Canada. It shall not be altered, distributed beyond its intended audience, produced, reproduced or published, in whole or in any substantial part thereof, without the express permission of CSE

Cat. No. D97-1/00-141-2022E-PDF
ISBN 978-0-660-41543-7

HOW CAN I PROTECT MY...?

PERSONAL 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 disable 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.

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.

PERSONALIZED QR CODES

- Keep your personalized QR codes (e.g. proof of vaccination, boarding pass) in a secure folder on your device.
- Allow your code to be scanned only by a secure and verified application (e.g. provincial government proof of vaccination app).

AVOID

- Enabling your devices to automatically execute the QR code action.
- Scanning a QR code posted in a public setting (e.g. in a public transit station or advertisements on the street).
- Scanning a QR code if it is 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.

PROOF OF VACCINATION

The Government of Canada has supported the provinces and territories to implement a standardized proof of vaccination using QR codes. The proof of vaccination can be used domestically to gain access to indoor establishments such as restaurants, sporting venues, and movie theatres. It can also be used for international travel.

The proof of vaccination includes a SMART Health Card QR code which contains some personal information, including your name, date of birth, and your COVID-19 vaccine history (date of vaccination, vaccine name, and number of doses received). Your name and date of birth from the proof of vaccination are matched with government-issued photo identification. The QR code enables timely processing as well as the validation of a digital signature to detect forgeries.

By following the tips listed above to secure your devices, protect your information, and practice cyber security when scanning or creating QR codes, you can protect the sensitive information contained in your vaccination records and other personalized QR codes.

© Government of Canada
This document is the property of the Government of Canada. It shall not be altered, distributed beyond its intended audience, produced, reproduced or published, in whole or in any substantial part thereof, without the express permission of CSE