Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Quick Response Codes in a COVID-19 Environment

NOVEMBER 2020

Introduction

Quick Response (QR) codes have increased in popularity in the COVID-19 environment, aiding contact tracing and business check-in efforts. This guide provides information for individuals and businesses to help protect against cyber threats when using QR codes.

Quick Response codes

What are Quick Response codes?

QR codes are similar to barcodes. They contain information that can be read by the camera or another app on your smartphone, triggering your smartphone to perform an action such as:

- visiting a website
- installing an app
- joining a Wi-Fi network
- adding someone's details to your contact list
- dialling a specified phone number
- sending a SMS/text message or an email to a specified recipient.

Scanning the above QR code directs you to the website https://www.cyber.gov.au

How are Quick Response codes being used in the COVID-19 environment?

QR codes are used for check-in at businesses to provide a quick way to collect customer contact details required by State and Territory governments for contact tracing, and are a contactless alternative to pen and paper.

Some businesses also display QR codes that direct customers to a website containing information such as the menu to avoid the need to sanitise printed copies between customers.

What are the risks of using Quick Response codes?

Scanning a QR code which directs you to a non-government website requesting your name, phone number and email address, could result in your personal contact information being used for marketing or criminal purposes. Additionally, it is quick and easy for criminals to generate QR codes as part of attempts to obtain your personal information, usually by causing your smartphone to visit a harmful website, install a malicious app or join an untrustworthy Wi-Fi network.

In contrast, there is a relatively lower risk when using an app developed by a State or Territory government to scan a check-in QR code provided:

- the app ignores QR codes that could result in your smartphone performing the actions previously listed
- your contact details are provided to the State or Territory government, not to the business
- details of your check-ins are deleted after a limited time period such as 28 days.

Using Quick Response codes

Guidance for individuals

If the business is in a State or Territory whose government has developed a check-in app, as have ACT[1] and NSW[2] at the time of publication of this document, install and use this app to scan the check-in QR code. If the business hasn't signed up to their government-provided check-in process, ask the business why not.

If there are no government-provided check-in apps for the State or Territory where the business is located, if the business hasn't signed up to use government-provided check-in apps or if you want to scan a QR code to view a restaurant's menu:

- Only scan QR codes located in prominent positions in the business, to reduce the likelihood of scanning malicious QR codes placed by someone other than their employees – if you're in doubt, ask an employee.
- While scanning a QR code, look for prompts on your smartphone indicating actions that the QR code will perform.
- Be ready to cancel or terminate an unwanted action triggered by scanning the QR code. For example, close your web browser if you are directed to an unknown website, or hang up if an unexpected phone call is initiated.
- During check-in, ask the business for their privacy policy detailing how your personal contact information will be collected, stored, used and deleted. Provide only the minimum amount of personal contact information required by the State or Territory government, such as your name and either your email address or phone number.

Guidance for businesses

If your State or Territory government has developed a check-in app, as have ACT and NSW at the time of publication of this document, sign up so that your customers can use it. Place the government-provided QR code in a prominent position within your business so that customers know to use the government-provided app to scan it. This helps avoid customers using their camera app to scan a malicious QR code placed in your business by someone other than your employees.

If there are no government-provided check-in apps for your State or Territory, the following steps can help to protect your customers:

- Refer to the Office of the Australian Information Commissioner's guidance for businesses that have obligations under the ***Privacy Act 1988*** in regards to collecting personal information for contact tracing[3] and follow it to ensure that customers' personal information is only used for contact tracing purposes. If a third-party vendor is used, ensure they are trusted providers. If possible, validate third-party privacy agreements and measures for

[1] https://www.covid19.act.gov.au/business-and-work/check-in-cbr

[2] https://www.service.nsw.gov.au/transaction/check-covid-safe-business-service-nsw-app

[3] https://www.oaic.gov.au/privacy/guidance-and-advice/guidance-for-businesses-collecting-personal-information-for-contact-tracing

capture and storage of customers' personal information, and ensure it is in compliance with your State or Territory's data processing policies.

- Only collect the minimum amount of customer contact information required by your State or Territory government, such as name and either email address or phone number, and delete this as soon as government rules allow (e.g. after 28 days in the ACT).
- Be transparent with customers regarding how their contact information is collected, stored, used and deleted.
- When generating a QR code that directs customers to a website:
    - avoid using services that shorten and obscure the website address
    - test the QR code before providing it to your customers to check if you are directed to the correct website
    - provide a screenshot and description of the website so that customers know what to expect in order to help avoid them being misdirected to a different website.
- Place the QR code in a prominent position and regularly check that it hasn't been replaced with a malicious QR code.

Further information

The Australian Cyber Security Centre's step-by-step guides to turning on automatic updates for smartphone operating systems, and turning on multi-factor authentication, can help to mitigate the harm caused by scanning a malicious QR code. They can be found at https://www.cyber.gov.au/acsc/small-and-medium-businesses/step-by-step-guides.

Contact details

If you have any questions regarding this guidance you can contact us via 1300 CYBER1 (1300 292 371) or https://www.cyber.gov.au/acsc/contact.