# Quick Response (QR) code

Fact Sheet

NSW
GOVERNMENT

## What is a QR code?

A QR code is a type of square barcode made up of a grid of black and white squares. It allows users to quickly access resources, authenticate services or make payments. QR code usage surged during COVID-19 due to its convenience and widespread acceptance, making it easy to check in to locations. QR codes can be scanned using a device's camera or a specific app, which then opens a web browser to access the linked content. There are two types of QR codes:

### Static QR codes

Fixed codes that always direct users to the same content

### Dynamic QR codes

Editable codes that can be updated after being generated, allowing changes to the linked content.

## Benefits

QR codes allow users to instantly access resources with a simple scan, leading to a wide range of uses from viewing menus to completing business surveys. Key benefits include:

- ✓ **cost-effective** – QR codes are typically free or inexpensive to generate
- ✓ **easy to implement** – QR codes can be easily created using online tools that don't require technical expertise
- ✓ **quick access** – provides users with immediate access to information or services linked to the code
- ✓ **standardised** – QR codes are universally recognised and can be scanned by any modern smartphone, making them widely accessible.

## Security considerations and risks

While QR codes are convenient, they also pose certain cyber security risks. Similar to URL shorteners, QR codes can be exploited for malicious purposes. Key risks include:

- ⊗ **malicious URL embedding** – scanning a QR code may lead to the download of malware or other harmful software
- ⊗ **phishing (quishing)** – QR codes can direct users to fraudulent websites designed to steal login credentials, personal information or financial data
- ⊗ **QRLJacking (Quick Response Code Login Jacking)** – a technique where attackers manipulate the 'Login with QR Code' feature by tricking users into scanning a legitimate QR code on a phishing site, allowing them to hijack accounts
- ⊗ **data leakage** – once scanned, QR codes may collect and track personal data that can be used without the user's knowledge for marketing or malicious purposes.

# Best practices for QR code safety

## For users

**Stay vigilant** – only scan QR codes from trusted sources. Avoid unknown or suspicious codes.

**Verify before scanning** – always ensure the QR code is legitimate and not altered or unusual.

**Be cautious of urgency** – malicious actors may create a false sense of urgency. Take time to think before acting.

**Avoid sharing sensitive information** – do not enter personal or financial details on sites accessed via unfamiliar QR codes.

**Keep devices updated** – regularly update your mobile device's operating system and apps to protect against vulnerabilities.

**Think before you click** – if the URL shown looks suspicious, don't click through. Head to the official website instead.

## For organisations

**Educate users** – provide training on identifying suspicious QR codes and reporting them.

**Use reputable QR code generators** – to minimise tampering risks and enable branding, only use reputable QR code generators.

**Monitor QR code use** – regularly check deployed QR codes for any signs of tampering or misuse.

**Ensure secure communication** – verify that the URLs linked to QR codes use TLS/SSL encryption.

**Set expiration dates** – implement expiry times for dynamic QR codes to prevent unauthorised reuse.

# Signs of a suspicious QR code

- Malicious actors may alter existing QR codes by placing a different QR code over the original, which can sometimes be seen or felt.
- Check if the QR code is poorly misaligned or there are spelling mistakes on the signage.
- Check if the QR code lacks information or context on how the it will be used or where it will direct you.
- If a file downloads immediately after scanning a QR code, do not install it and contact your IT team.

## Contact us

**For more information, please contact Cyber Security NSW:**
**info@cyber.nsw.gov.au**