



## Chinese use of QR codes

QR codes, an abbreviation of Quick Response codes, have existed since 1994.

In 2000, international standards were published, and QR codes became widely available.



QR codes are a method of "barcoding" a string of data. They can be used for websites, email addresses, app addresses, WeChat, and many more.

At the outset, QR codes were not widely used in Western countries. Sharing a small amount of data by voice, email, text, etc., was straightforward: "Our website is [www.accesstochina.com](http://www.accesstochina.com)." My email address is [support@accesstochina.com](mailto:support@accesstochina.com).

Typically, there is a simple assumption that we all speak English and use the Latin alphabet!

That is only sometimes the case. For example;

مرحبا, γεια σας, 你好, Привет

In the early 2000s, China embarked on a technological revolution. As this technology became accessible to the general public, the use of Latin characters posed a challenge. While small Latin words used in Pinyin were manageable, long, nonsensical strings of Latin characters in a foreign language were difficult to comprehend, spell, or transcribe.

A more significant issue was passwords. Given the problem with using Latin characters, many Chinese passwords were short and were changed only occasionally.

Chinese social media platforms ingeniously tackled the language barrier by employing QR codes. When scanned, these codes provide access to services through embedded, long, and complex passwords. Consequently, QR code scanning has become ubiquitous among Chinese social media users.

Because most Chinese social media users are familiar with QR codes, they are widely used in China.

Today, QR codes are ubiquitous in China. They have replaced domain names in marketing and sales, and businesses and people have replaced the writing of their internet links with QR codes.



<https://www.accesstochina.com>

Today, QR codes are ubiquitous in China. For example;

- Website
- Internet login/passwords
- Supermarket
- Billboard adverts
- Information displays

QR codes have also replaced the printing of URLs, email addresses, and social media handles on business cards.

Here are a few examples:



A QR code can be in different colours and styles, with or without logos embedded in the centre.

QR codes have a significant advantage over barcodes in that they are flexible and can store a broader range of data types and volumes.

Given that people no longer have to type the URL, you can add additional information to the URL to track the inquiry source, e.g., use different URLs on brochures, websites, promotions, etc. You can also track the use of your QR codes.

At present, QR codes are prevalent in China and are increasingly used worldwide.

Are there a few problems?

- Outside China, not everyone uses, knows, or has a QR scanner on their Mobile Phone. Your URL must still be printed on brochures, business cards, and similar materials.
- The longer the URL, passwords, etc., the more complex the QR code. This can make it too large to be read successfully.
- The QR code colour must contrast with the background colour. A QR code is successfully scanned if there is a sharp contrast between the background and the QR code colour. For example, the image on the Access to China homepage (<https://www.accesstochina.com>) features a black QR code in the top-right corner. This is not our regular QR code; see above. The change was necessary to ensure it could be read successfully.
- When creating a QR code, add <http://> or <https://> to the front of the website, e.g., <http://www.accesstochina.com>, or for email, <mailto:support@accesstochina.com>.
- You must test your QR code before publishing. Many problems with QR codes can be resolved at the outset through a few simple tests.

#### **Access to China QR code recommendations.**

- Create QR codes and publish them on all marketing materials, business cards, etc.
- Add your QR code(s) to your company website's home page. In China, readers often transfer web content from desktops to mobile devices; a QR code facilitates this process.
- Use different URL codes to track business sources such as Brochures, Business cards, and websites.
- Always check and test that QR codes are working both for seeing the website and the tracking system.
- Do not use a lengthy URL or email address, as the QR code becomes too complex and challenging for QR scanners to read.

We recommend using free QR code generators to understand how they work and what design characteristics are appropriate for your business. QR code design companies are available on the internet if you need assistance.

If you want to create a QR code, you can find many free tools online to generate it, e.g., <https://www.unitag.io/qrcode>.

## QR code scams – warning

Today, QR codes are essential for consumers and businesses in information and transaction flows. As with most things, QR codes are vulnerable to scams.

While I am sure this is occurring in China, it is a global problem.

QR code scams are a growing concern as QR codes become more prevalent for everything from payments to website access. Scammers use QR codes to exploit people's trust and the ease of use by tricking them into scanning malicious links that lead to harmful actions. This is the same type of scam you see in Emails. For example, you receive an email that appears to be from your bank, but it's not, and the links within the email lead to a fraudulent website.

Here's how these scams typically work and how to avoid them:

- **Phishing URLs:** Scammers create or replace QR codes that, when scanned, direct users to fake websites designed to steal personal information, such as login credentials, banking details, or social security numbers.
- **Malicious Downloads:** The QR code can link to malware that downloads onto a user's device, potentially stealing sensitive data or controlling the device remotely.
- **Payment Scams** - In financial scams, scammers replace legitimate QR codes (for example, on parking meters or donation sites) with fraudulent ones. Scanning these codes may lead to fraudulent payment portals through which users unwittingly transfer money to criminals.
- **Fake Customer Service:** Scammers post QR codes in public places or online forums, advertising fake customer service numbers or websites. Scanning the code may result in fraudulent support chats or calls in which personal information is requested.
- **Fake Promotions or Free Offers:** Scammers often use QR codes in advertisements or posters claiming to offer free products, services, or gifts. Scanning the code can lead users to phishing pages or require them to enter personal information under false pretences.

### Examples of Common QR Code Scams

**Fake Payment Codes:** These are found on receipts, restaurant tables, or parking meters, where users scan to make payments, but the funds are diverted to scammers.

**Tampered QR Codes:** Legitimate posters or business signs are overlaid with fraudulent QR codes.

**Scam Emails or Texts:** Scammers send messages purporting to be from legitimate companies and include a QR code for "account verification" or "updating information."

### How to Protect Your Business

- Make your staff aware of the QR scams.
- Check your business's QR codes to see if they have been replaced with scam codes.
- Check the products and services, packaging, brochures, etc., for scam QR codes and continue to do this.
- Add to your purchasing agreements that suppliers have checked products, etc., and have checked for scam QR codes. This will increase awareness of the problem and, in turn, reduce the opportunity for QR scams.

## How to Protect Yourself

- Check the Source - Only scan QR codes from trusted sources. If you encounter a QR code on a flyer, poster, or email, verify its authenticity by contacting the company or individual.
- Preview the URL - When scanning a QR code, most phones preview it before opening it. Before proceeding, check whether the URL appears suspicious (e.g., misspellings, unusual domains).
- Use a QR Code Scanner with Security Features - Some QR code scanning apps offer security features that warn you if the QR code leads to a suspicious or unsafe link.
- Avoid Public or Unverified Codes - Be cautious of QR codes in public places, as they can easily be tampered with. Always verify the code's legitimacy before scanning.
- Watch for Overlays - Scammers may place fake QR codes over legitimate ones. Check whether a QR code appears to have been tampered with or covered.
- Use Anti-Malware Software - Ensure your smartphone or device has security software that can detect and block malicious sites or malware that may come from QR code links.
- Don't Enter Personal Info After Scanning - Be extremely cautious if a QR code directs you to a website that asks for personal information (like your social security number, credit card information, or login details). Double-check the site's URL and legitimacy.
- Avoid QR Code Payments without Verification - If paying via a QR code, verify directly with the merchant or service provider to ensure the code belongs to them.