How to Tell if a QR Code Is Safe Before Opening It (Quishing Guide)

QR code phishing — known as quishing — is a growing threat. Learn the red flags to spot before you scan, and what to check after scanning before you tap Open.

Author: Lubor Šimůnek · Published: August 23, 2026 · Security
Online version: https://appstoryo.com/en/blog/qr-code-safe-quishing-guide



What Is Quishing?

Quishing is QR code phishing. Attackers print or display a QR code that, once scanned, sends you to a malicious website designed to steal your credentials, install malware on your device, or present a fake payment page. The name is a blend of 'QR' and 'phishing,' and it is one of the fastest-growing social-engineering attacks because most people trust QR codes without thinking twice.

Why QR Codes Are a Unique Risk

With a regular link in an email you can at least hover over it and read the URL before clicking. With a QR code you cannot see the destination until your scanner decodes it — and even then many default camera apps open the browser immediately without showing you the address first. That split second is all a malicious site needs to begin tracking your device or triggering a download.

QR codes also bypass email spam filters entirely. Filters scan for suspicious text and known-bad URLs, but an image of a QR code contains neither — it looks like a perfectly innocent picture. This is why phishing emails increasingly replace their old hyperlinks with QR codes, especially in attacks targeting corporate employees.

Real-world quishing is everywhere: stickers pasted over legitimate codes on parking meters, fake restaurant menus printed with a slightly different code, parcel-delivery scam notices left in letterboxes, and fake public charging station instructions that prompt you to 'scan to pay.'

Red Flags to Check BEFORE You Scan

- **Sticker over an original code.** A QR sticker placed on top of an existing code is a classic swap. Tug the corner gently — if it peels off, do not scan it.
- **Urgency language on a random flyer.** 'Scan now to claim your prize,' 'Act within 24 hours,' or 'Your parcel is held — scan to reschedule' are pressure tactics designed to stop you from thinking.
- **Unsolicited mail or email.** A letter or email you did not expect, with a QR code as the main call to action, is a strong warning sign — especially if it claims to be from a bank, delivery company, or government agency.
- **No visible branding context.** A code floating alone on a wall with no company name, no URL hint, and no explanation of where it leads should be treated with suspicion.

What to Check AFTER Scanning but BEFORE Tapping Open

This is the most important moment. When your scanner shows you the decoded URL, pause and read it carefully before you proceed.

- **Does the domain match who you expect?** If you scanned a code at a HSBC ATM, the URL should be on an hsbc.com domain, not hsbc-secure-login.net or any other variation.
- **Is it a URL shortener?** Links that begin with bit.ly, tinyurl.com, t.co, or similar shortening services hide the real destination. A shortener is not automatically malicious, but it removes your ability to verify the endpoint before visiting. Use a URL-expander service (search for 'URL expander' in your browser) to reveal the true address first.
- **Misspelled or lookalike domains.** Attackers register domains like paypa1.com (number one instead of letter L), g00gle.com (zeros instead of letter O), or app1e.com. Read every character carefully.
- **Random subdomains on unfamiliar roots.** Something like login.secure.amazon-parcels-uk.com looks plausible at first glance, but the actual domain (the part just before the first single slash) is amazon-parcels-uk.com — not amazon.com.
- **Unexpected country-code domains used as redirects.** Domains ending in .tk, .ml, .ga, or .cf are frequently used in free phishing infrastructure.

Safe Habits to Build Now

Only scan codes from sources you physically trust — a menu handed to you by a waiter in a restaurant you chose, a poster at an event you are attending, or a product you purchased. Never enter login credentials, card numbers, or personal details on a page you reached by scanning a QR code in an unsolicited email or letter. When in doubt, navigate to the service directly by typing the address into your browser.

How QR Code Reader Without Ads Helps

One practical layer of protection is to use a scanner that shows you the full URL preview before it opens anything. QR Code Reader Without Ads does exactly that: every scan surfaces the complete destination URL on screen, giving you a clear moment to read and decide before any browser action is taken. If the URL looks wrong, you simply do not tap Open — no harm done.

The app also keeps a local scan history on your device, so if you later suspect a code you scanned, you can go back and check the URL. Crucially, it collects no data and shows no ads, which means your scanning behaviour is not being tracked or monetised by a third party. You can find it on the App Store (search 'QR Code Reader Without Ads') or on Google Play.

Quishing is a low-effort, high-reward attack for criminals precisely because people are conditioned to trust QR codes. Slowing down for two seconds to read the URL preview is one of the simplest and most effective security habits you can develop.

Download QR Code Reader Without Ads free for iOS or Android — no ads, no tracking, and it works fully offline.

Cite as: Lubor Šimůnek (2026). *How to Tell if a QR Code Is Safe Before Opening It (Quishing Guide)*. AppStoryo, lapnito.cz s.r.o.. https://appstoryo.com/en/blog/qr-code-safe-quishing-guide
© 2026 lapnito.cz s.r.o.