如何在開啟 QR 碼前判斷是否安全（Quishing 防詐指南）

QR 碼網路釣魚（Quishing）正在迅速蔓延。了解掃描前的危險信號及掃描後點擊「開啟」前應檢查的內容。

作者: Lubor Šimůnek • 發佈日期: August 23, 2026 • 安全

線上版本: https://appstoryo.com/zh-hant/blog/qr-code-safe-quishing-guide



什麼是 Quishing?

Quishing 是透過 QR 碼實施的網路釣魚攻擊。攻擊者製作一個 QR 碼，掃描後會將用戶引導至惡意網站，目的是竊取帳號密碼、安裝惡意軟體或呈現偽造付款頁面。這個詞由「QR」和「phishing（釣魚）」合成，由於人們幾乎不加思索地信任 QR 碼，此類攻擊正在快速增長。

QR 碼為何具有特殊風險

對於普通連結，可以將滑鼠懸停查看 URL 後再決定是否點擊。但 QR 碼在掃描器解碼前無法看到目標地址——許多相機應用程式會直接開啟瀏覽器而不顯示網址。就在這短暫瞬間，惡意網站已可能開始追蹤您的裝置。

QR 碼還能完全繞過垃圾郵件過濾器。過濾器會掃描可疑文字或已知惡意 URL，但 QR 碼圖片看起來完全無害。正因如此，網路釣魚郵件越來越多地以 QR 碼取代超連結，尤其是針對企業員工的攻擊。

現實生活中，Quishing 常見於：貼在停車收費機合法 QR 碼上的貼紙、偽造的餐廳菜單、投入信箱的快遞詐騙通知，以及要求「掃碼付款」的虛假公共充電站。

掃描前需注意的危險信號

- 貼在原始 QR 碼上的貼紙。貼在另一個 QR 碼上的貼紙是典型的替換手法。輕輕掀起一角——若能揭

開，請勿掃描。

- 陌生傳單上的緊迫性語言。「立即掃描領取獎品」或「您的包裹遭扣押——掃碼重新安排配送」是施壓手段。
- 未經請求的郵件或信函。來自銀行、快遞公司或政府機關的意外通知，以 QR 碼作為主要行動號召，是強烈的警示信號。

掃描後、開啟前需檢查的內容

- 網域是否符合預期？如果您在銀行掃描了 QR 碼，URL 應位於官方網域上。
- 是否使用了短網址服務？bit.ly 或 tinyurl.com 等服務隱藏了真實目標地址。訪問前請使用 URL 展開服務查看真實地址。
- 拼寫錯誤或仿冒網域。注意 paypa1.com（用數字 1 取代字母 L）或 g00gle.com（用數字 0 取代字母 O）。仔細閱讀每個字元。
- 可疑子網域。login.secure.amazon-delivery-tw.com 看似合法，但真實網域是 amazon-delivery-tw.com，而非 amazon.com。

QR Code Reader Without Ads 如何提供協助

QR Code Reader Without Ads 在開啟任何內容前會顯示完整的 URL 預覽，讓您有時間檢視連結後再做決定。若地址看起來可疑，只需不點擊「開啟」即可。該應用程式在您的裝置上本地儲存掃描記錄，不收集資料，也不顯示廣告。請在 App Store 或 Google Play 搜尋「QR Code Reader Without Ads」。

立即在 iOS 或 Android 上免費下載 **QR Code Reader Without Ads**——無廣告、無追蹤，完全離線運作。

引用格式: Lubor Šimůnek (2026). 如何在開啟 *QR* 碼前判斷是否安全（*Quishing* 防詐指南）. AppStoryo, lapnito.cz s.r.o.. https://appstoryo.com/zh-hant/blog/qr-code-safe-quishing-guide
© 2026 lapnito.cz s.r.o.