# كيف تعرف إذا كان رمز QR آمناً قبل فتحه (دليل مكافحة Quishing)

Quishing هو التصيد الاحتيالي عبر رموز QR. تعرّف على العلامات التحذيرية قبل المسح وما يجب التحقق منه قبل النقر على فتح.

الكاتب: Lubor Šimůnek · تاريخ النشر: August 23, 2026 · الأمان
النسخة الإلكترونية: https://appstoryo.com/ar/blog/qr-code-safe-quishing-guide




## ما هو Quishing؟

Quishing هو التصيد الاحتيالي باستخدام رموز QR. ينشئ المهاجم رمزاً يؤدي مسحه إلى موقع خبيث مصمم لسرقة بيانات اعتماد المستخدم أو تثبيت برامج ضارة أو عرض صفحة دفع مزيفة. يجمع المصطلح بين 'QR' و'phishing'، وينتشر هذا النوع من الهجمات بسرعة لأن الناس يثقون في رموز QR دون تفكير.

## لماذا تشكّل رموز QR خطراً خاصاً

مع الروابط العادية يمكنك تمرير المؤشر فوقها لرؤية العنوان قبل النقر. أما مع رمز QR فلا يمكنك رؤية الوجهة حتى يفكّ الماسح ترميزه — وكثير من تطبيقات الكاميرا تفتح المتصفح فوراً دون عرض العنوان. تلك اللحظة كافية لموقع خبيث لبدء تتبع جهازك.

تتجاوز رموز QR أيضاً فلاتر البريد العشوائي تماماً؛ فالفلاتر تبحث عن نصوص مشبوهة أو عناوين URL ضارة معروفة، لكن صورة رمز QR تبدو بريئة تماماً. لهذا تستبدل رسائل التصيد الاحتيالي روابطها القديمة بشكل متزايد برموز QR، خاصة في الهجمات الموجهة للشركات.

في الحياة اليومية يظهر Quishing في ملصقات فوق رموز شرعية على عدادات الانتظار، وقوائم طعام مزورة، وإشعارات طرود احتيالية في صناديق البريد، ومحطات شحن عامة مزيفة تطلب 'المسح للدفع'.

## العلامات التحذيرية قبل المسح

- **ملصق فوق رمز أصلي.** ملصق QR مُلصق فوق رمز آخر هو استبدال كلاسيكي. ارفع الزاوية برفق — إن انفصل فلا تمسح.
- **لغة استعجالية على منشور مجهول.** 'امسح الآن للفوز بجائزتك' أو 'طردك محتجز — امسح لإعادة الجدولة' هي أساليب ضغط نفسي.
- **بريد إلكتروني أو رسالة غير مطلوبة.** اتصال غير متوقع من بنك أو شركة شحن أو جهة حكومية تستخدم رمز QR كدعوة رئيسية للتصرف هو تحذير قوي.

## ما يجب التحقق منه بعد المسح وقبل الفتح

- **هل النطاق يطابق توقعاتك؟** إذا مسحت رمز QR في أحد البنوك يجب أن يكون عنوان URL على النطاق الرسمي.
- **هل هو مختصر روابط؟** خدمات مثل bit.ly أو tinyurl.com تخفي الوجهة الحقيقية. استخدم خدمة توسيع الروابط لمعرفة العنوان الفعلي قبل الزيارة.
- **نطاقات مكتوبة بأخطاء أو مُشابِهة.** انتبه لـ paypa1.com (رقم 1 بدلاً من حرف L) أو g00gle.com (أصفار بدلاً من حرف O). اقرأ كل حرف بعناية.
- **نطاقات فرعية مشبوهة.** login.secure.amazon-delivery-sa.com يبدو شرعياً، لكن النطاق الفعلي هو amazon-delivery-sa.com وليس amazon.com.

## كيف يساعد تطبيق QR Code Reader Without Ads

يعرض تطبيق QR Code Reader Without Ads عنوان URL الكامل قبل فتح أي شيء، مما يمنحك لحظة لفحص الرابط قبل اتخاذ أي إجراء. إذا بدا العنوان مشبوهاً، فلا تنقر ببساطة على 'فتح'. يحتفظ التطبيق بسجل مسح محلي على جهازك، ولا يجمع أي بيانات ولا يعرض أي إعلانات. ابحث عنه في App Store أو Google Play باسم 'QR Code Reader Without Ads'.

**حمّل QR Code Reader Without Ads مجانًا لأجهزة iOS أو Android** — بلا إعلانات، وبلا تتبّع، ويعمل دون اتصال بالإنترنت تمامًا.

**طريقة الاقتباس:** Lubor Šimůnek (2026). كيف تعرف إذا كان رمز QR آمناً قبل فتحه (دليل مكافحة Quishing). AppStoryo, https://appstoryo.com/ar/blog/qr-code-safe-quishing-guide. lapnito.cz s.r.o.
© 2026 lapnito.cz s.r.o.