مزيفة لتوجيه الضحايا إلى مواقع وهمية، سرقة QR هو تصيد يستغل رموز (Quishing) الاحتيال عبر رموز الاستجابة السريعة بياناتهم، أو زرع برامج ضارة. خطورته تكمن في عدم قدرة العين البشرية على كشف تزوير الرمز، مما يمنح المحتالين فرصة وهمية فوق رموز الدفع الأصلية، وإرسال QR مثالية. تتعدد أساليب الاحتيال الشائعة، منها إنشاء إعلانات مزيفة، لصق رموز رسائل أو بريد إلكتروني زائف حول شحنات/فواتير/طرود تتطلب مسح الرمز. كما يستخدم المحتالون ملصقات عامة توهم بهدايا أو خصومات، أو إشعارات بجوائز كبرى، وحتى انتحال صفة البنوك عبر "واتساب" لطلب تحديث بيانات بمسح رمز. كل هذه الحيل تستغل الإلحاح لدفع الضحايا للمسح وفتح الروابط دون تفكير. للوقاية، تحقق من صحة المواقع وأي أخطاء إملائية. في المرسلة عبر الرسائل أو وسائل QR الأماكن العامة، مرر إصبعك على الرمز للتأكد من عدم وجود ملصق مزيف. لا تمسح رموز قد يتسبب في إرسال أموال من QR التواصل الاجتماعي أو البريد الإلكتروني لحل مشكلات الحساب. تذكر دائمًا أن مسح رمز حسابك، لا استقبالها.