الاحتيال عبر رموز الاستجابة السريعة (Quishing) هو تصيد يستغل رموز QR مزيفة لتوجيه الضحايا إلى مواقع وهمية، سرقة بياناتهم، أو زرع برامج ضارة. خطورته تكمن في عدم قدرة العين البشرية على كشف تزوير الرمز، مما يمنح المحتالين فرصة مثالية. تتعدد أساليب الاحتيال الشائعة، منها إنشاء إعلانات مزيفة، لصق رموز QR وهمية فوق رموز الدفع الأصلية، وإرسال 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 الأماكن العامة، مرر إصبعك على الرمز للتأكد من عدم وجود ملصق مزيف. لا تمسح رموز QR المرسلة عبر الرسائل أو وسائل التواصل الاجتماعي أو البريد الإلكتروني لحل مشكلات الحساب. تذكر دائمًا أن مسح رمز QR قد يتسبب في إرسال أموال من حسابك، لا استقبالها.

lakhasly.com © تم تلخيص النص بواسطة موقع لخصلي