Cómo Saber si un Código QR Es Seguro Antes de Abrirlo (Guía Anti-Quishing)

El quishing es la modalidad de phishing que usa códigos QR. Aprende a detectar señales de alerta antes y después de escanear para no caer en la trampa.

Autor: Lubor Šimůnek · Publicado: August 23, 2026 · Seguridad
Versión en línea: https://appstoryo.com/es/blog/qr-code-safe-quishing-guide



¿Qué es el quishing?

El quishing es phishing a través de códigos QR. Un atacante coloca un código que, al escanearse, lleva a una página falsa diseñada para robar credenciales, instalar malware o simular un pago. La palabra combina 'QR' y 'phishing', y su popularidad crece porque la gente confía en los QR casi de forma automática.

Por qué los códigos QR son un riesgo especial

Con un enlace normal puedes pasar el ratón por encima y ver la URL antes de hacer clic. Con un QR no puedes ver el destino hasta que tu escáner lo decodifica, y muchas aplicaciones de cámara abren el navegador de inmediato sin mostrarte la dirección. Ese instante es suficiente para que un sitio malicioso comience a rastrear tu dispositivo.

Además, los QR evitan los filtros de spam del correo: un filtro busca texto sospechoso o URLs conocidas como dañinas, pero una imagen de código QR parece completamente inofensiva. Por eso cada vez más correos de phishing reemplazan sus hipervínculos por QR, especialmente en ataques corporativos.

En el mundo real el quishing aparece en pegatinas sobre códigos legítimos en parquímetros, menús de restaurante falsificados, avisos de entrega de paquetes dejados en el buzón, o

instrucciones en estaciones de carga públicas falsas que piden 'escanear para pagar'.

Señales de alerta ANTES de escanear

- **Pegatina sobre un código original.** Un QR pegado encima de otro es un intercambio clásico. Levanta la esquina: si se despega, no lo escanees.
- **Lenguaje de urgencia en un folleto desconocido.** 'Escanea ahora para reclamar tu premio' o 'Tu paquete está retenido, escanea para reprogramar' son tácticas de presión.
- **Correo o carta no solicitado.** Una comunicación inesperada de un banco, empresa de mensajería o entidad gubernamental que usa un QR como llamada a la acción principal es una señal de alerta importante.

Qué comprobar DESPUÉS de escanear y ANTES de abrir

Este es el momento más crítico. Cuando tu escáner muestra la URL decodificada, lee con atención antes de continuar.

- **¿Coincide el dominio con lo esperado?** Si escaneaste un QR en un banco, la URL debe estar en el dominio oficial, no en una variación extraña.
- **¿Es un acortador de URLs?** Servicios como bit.ly o tinyurl.com ocultan el destino real. Usa un expansor de URLs para revelar la dirección verdadera antes de visitar.
- **Dominios mal escritos o similares.** Fíjate en paypa1.com (número uno en lugar de la letra L) o g00gle.com (ceros en lugar de la letra O). Lee cada carácter con cuidado.
- **Subdominios sospechosos.** login.secure.amazon-paquetes-es.com parece legítimo, pero el dominio real es amazon-paquetes-es.com, no amazon.com.

Cómo ayuda QR Code Reader Without Ads

QR Code Reader Without Ads muestra la URL completa antes de abrir cualquier enlace. Eso te da el momento necesario para leer y decidir. Si la URL parece sospechosa, simplemente no tocas 'Abrir'. La aplicación guarda un historial local de escaneos en tu dispositivo, no recopila datos y no muestra anuncios. Disponible en el App Store y en Google Play buscando 'QR Code Reader Without Ads'.

Descarga QR Code Reader Without Ads gratis para iOS o Android: sin anuncios, sin rastreo y funciona completamente sin conexión.

Cómo citar: Lubor Šimůnek (2026). *Cómo Saber si un Código QR Es Seguro Antes de Abrirlo (Guía Anti-Quishing)*. AppStoryo, lapnito.cz s.r.o.. https://appstoryo.com/es/blog/qr-code-safe-quishing-guide
© 2026 lapnito.cz s.r.o.