

Los códigos QR están por todas partes, pero algunos pueden ser manipulados para engañarnos. La palabra QRishing surge de la combinación de códigos QR (”quick response” o respuesta rápida) y phishing (conocida modalidad de fraude digital).

Es una técnica usada por ciberdelincuentes para manipulan códigos QR y engañar a las víctimas. Al escanearlos, redirigen a sitios falsos que parecen legítimos con el objetivo de robar información sensible o inducir a la instalación de malware.

Los atacantes aprovechan estos códigos para:

- Crear QRs que parecen legítimos, pero redirigen a sitios fraudulentos.
- Alterar los legítimos (por ejemplo, con stickers o cambios en los enlaces), ocultando su verdadero propósito.

¿Qué pasa cuando entrás en un sitio falso?

- Pueden pedirte datos personales o bancarios para robarlos.
- Puede descargarse un malware que, al instalarlo, comprometa el dispositivo.

Paso a paso del QRishing

- **Creación:** los atacantes crean o alteran un QR para que parezca legítimo.
- **Distribución:** lo colocan en lugares estratégicos o lo envían por medios digitales.
- **Engaño:** atraen víctimas con promociones falsas, facturas engañosas y otras técnicas de ingeniería social.
- **Robo de datos:** al escanear el QR e ingresar información en un sitio falso, los atacantes pueden capturarla.

- **Explotación:** usan esa información para fraudes financieros, robo de identidad o venderla en la dark web.

¿Escanear un QR falso instala un malware?

- El riesgo principal no está en el escaneo, sino en lo que el usuario haga después, como ejecutar un archivo peligroso o aceptar permisos.

¿Cómo evitar el QRishing?

- Revisar siempre el enlace antes de interactuar con un QR.
- Evitar escanear usando apps de terceros no verificadas.
- Configurar la cámara y apps para evitar que los enlaces se abran automáticamente.
- Verificar que el QR no provenga de fuentes desconocidas ni esté manipulado.
- Prestar atención al contexto y a los detalles.
- Desconfiar de enlaces acortados.
- Mantener el software del dispositivo actualizado.

Recordemos: los códigos QR son prácticos, pero pueden ser alterados fácilmente. Además, los falsos pueden parecer idénticos a los legítimos, lo que dificulta su detección a simple vista. Por eso, la clave está en verificar el enlace antes de interactuar.