CÓDIGOS QR: SON UN RIESGO PARA LA SEGURIDAD?

Por: 3+ Security Colombia

1. Los códigos QR son códigos de respuesta rápida (quick response en inglés), capaces de almacenar una gran cantidad de información.
2. Estos códigos se pueden escanear con un smartphone para acceder a la información que contienen.
3. Los códigos QR se generan a través de un software de creación de este tipo de códigos y están estandarizados por la Norma ISO/IEC 18004:2015.

32.8%

Usuarios de códigos QR realizaron pagos por este medio

USOS FRECUENTES

- Acceso a una red Wifi
- Descarga de aplicaciones
- Acceso a servicios (como whatsapp web)
- Entradas para acceder a medios de transporte, zonas vips o zonas de ocio
- Medio de pago
- Consultar menús o catálogos

PELIGROS DE LOS CÓDIGOS QR:

QR maliciosos

A través de la creación de un código QR malicioso, se puede dirigir a los usuarios a una web fraudulenta para llevar a cabo la siguiente fase del ataque como, por ejemplo enviar mensajes o correos electrónicos desde el móvil

Qrishing

Conjuga la ingeniería social con el escaneo de un código QR para llevar a los usuarios a una web falsa, que suplanta una web oficial, donde se le pedirá al usuario que facilite alguna de sus credenciales, para así poder robarlas.

Descarga malware

Busca conducir a los usuarios a una web de descarga de malware o de inyección de código malicioso, muchas veces a través de una descarga forzada de malware al visitar un sitio web.

Qrljacking

Es el secuestro de sesión, es decir, se usa el código QR para secuestrar la cuenta de un servicio que utilice la función de iniciar sesión con código QR.

Rastreo

Los códigos QR maliciosos también pueden usarse para rastrear las acciones del usuario cuando navega por Internet e, incluso, revelar su localización física.

WiFi comprometida

Puede servir para añadir una red WiFi maliciosa como una de confianza a la lista de redes inalámbricas del móvil, haciendo que el usuario se conecte pensando que es segura y dejando así acceso a su dispositivo y sus cuentas a los cibercriminales.

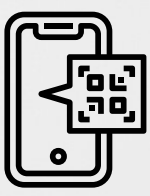
CLAVES PARA PROTEGER A SUS CLIENTES:

Compruebe regularmente que el código QR conduce a donde debe conducir y no a una web falsa.

Utilice un generador de códigos QR que ofrezca garantías y confianza en materia de seguridad.

Comprobar que el código QR no ha sido modificado ni le han puesto un sticker encima.

CLAVES PARA PROTEGERSE COMO USUARIO:



Utilice aplicaciones de escaneo que permitan ver la URL antes de abrirla

No escanear códigos QR de dudosa procedencia

Si ha accedido a una web, compruebe la URL antes de introducir ninguna credencial en ella.