LITORALPRESS

Fecha: 06-02-2025
Medio: El Mercurio
Supl. : El Mercurio - Cuerpo A
Tipo: Noticia general
Título: El código QR puede ser la puerta digital para que delincuentes roben datos o dinero

Pág. : 8
Cm2: 608,5

Tiraje: 126.654
Lectoría: 320.543
Favorabilidad: No Definida

Su uso se ha expandido a varios ámbitos de la vida cotidiana:

El código QR puede ser la puerta digital para que delincuentes roben datos o dinero

Están en la entrada de un concierto y también en el menú digital de un restaurante. Su masificación ha hecho que los *hackers* falsifiquen los códigos para que lleven a sitios fraudulentos que extraen datos importantes, incluso de tarjetas de crédito. Expertos explican cómo funciona y qué hacer para prevenir.

ALEXIS IBARRA O.

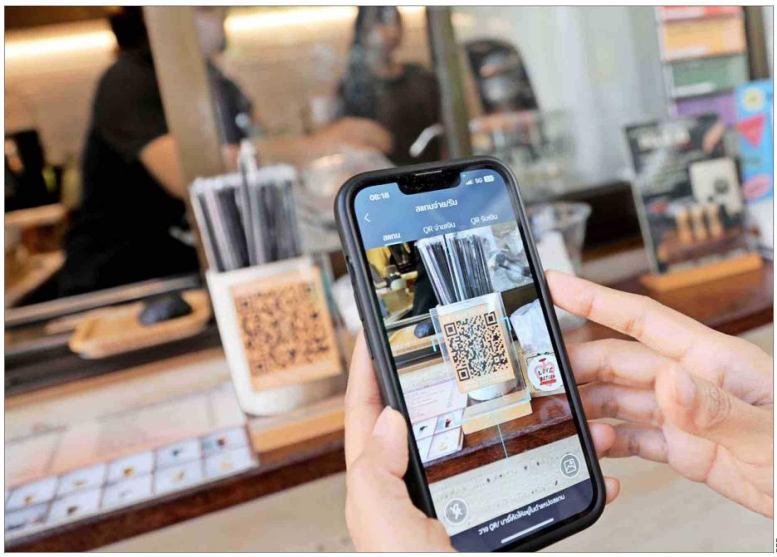
Consultar el menú de un restaurante, visitar la red social de una persona, validar las entradas a un concierto o el pago al subir a un bus del transporte público; incluso, para pagar en la web o en máquinas expendedoras. Los usos del código QR cada vez son más variados.

"Un código QR, en esencia, es un código de barra bidimensional que cuenta con un patrón característico: un cuadrado que dentro tiene cuadrados negros y blancos que contienen distinto tipo de información que es de acceso rápido y que puede ser escaneado fácilmente por la cámara de los celulares para acceder a dicha información", dice Leandro Cuozzo, analista de Seguridad en el Equipo Global de Investigación y Análisis para América Latina en Kaspersky.

Es que la simple acción de apuntar con la cámara del celular a este código para acceder a contenido y servicios que de otra forma se hace más engorroso ha universalizado su uso. Pero esa misma masividad lo ha convertido también en un elemento usado por ciberdelincuentes para robar datos y dinero.

"Son muchos los ciberdelincuentes que se aprovechan de ello para robar información sensible, descargar archivos maliciosos o para difundir información falsa, entre otras acciones malintencionadas", dice Francisco Fernández, gerente general de Avantic Chile.

Un *modus operandi* —agrega Rodrigo Hernández, gerente de Ciberseguridad de Entel— consiste en que estos códigos QR "redirigen a las víctimas a sitios web poco fiables donde se les solicita entregar datos personales, o realizar pagos fraudulentos a través de transferencias bancarias".



EFE

Los códigos QR de restaurantes son muy usados por los usuarios. Los ciberdelincuentes podrían reemplazarlos por sus propios códigos que llevan a un sitio que puede robar datos.

Existe el término *Quishing*, también conocido como *Phishing* QR, que "implica la creación por parte de un ciberdelincuente de un código QR que derive a las víctimas a un sitio *web* malicioso donde se les roba información, ya sea personal (como el RUT, credenciales, etc.), o bancaria (como contraseñas y datos de tarjetas de crédito o débito)".

De hecho, agrega Fernández, "algunos códigos QR utilizados en restaurantes, cafeterías, pequeños negocios, *retail*, y servicios públicos, por mencionar determinados lugares, pueden ser intervenidos por desconocidos para robar datos personales e información sensible". Basta con que el ciberdelincuente adhiera una pegatina con su propio código QR para concretar la trampa.

Otra forma de engaño que se ha visto en los países latinoamericanos, cuenta Cuozzo, es la aparición en la vía pública de carteles que dicen: '¿Quieres ver las fotos de la persona que me engañó?'. Alguien que es muy curioso escanea el QR "y en vez de encontrarse con fotos se encuentra con un *malware*".

Cuozzo describe otra forma de engaño: dejan pegado un papel en el auto, simulando ser una infracción y afirmando que a través del QR se puede acceder al detalle de la infracción y pagarla. Así los ciberdelincuentes pueden acceder a datos de la tarjeta de crédito.

También se usa como un código para acceder a una red *wifi* gratuita, "pero este *wifi* está controlado por un delincuente que podría estar escaneando toda la comunicación que realizas a través de esa red", precisa Cuozzo.

Cómo evitarlo

Lo primero es que antes de escanear, el usuario debe asegurarse de que el código provenga de una fuente fiable. "No se debe confiar en códigos colocados en espacios públicos sin confirmación", dice Hernández. Y agrega: "También se recomienda activar la revisión previa de URL: muchas aplicaciones de escaneo muestran la dirección a la que redirige el código QR. Es importante verificar que sea legítima antes de continuar y hacer clic".

"La regla de oro es evitar escanear cualquier QR con el cual te tropieces y del cual no sepas su origen, la fuente o qué contiene", dice Cuozzo. Y si se necesita escanear un QR, como es el caso del menú de un restaurante, hay que cerciorarse de que "efectivamente apunte al sitio del restaurante o uno de menús y que no apunte a cualquier otro lugar o que tenga un acortador de URL, ya que sería algo un poco sospechoso", añade el experto.

El especialista recalca la advertencia de no compartir información personal, confidencial o de la tarjeta de crédito en ningún sitio desconocido, y "menos en uno al que llegaste a través de un QR".