QRurb Your Enthusiasm 2021:

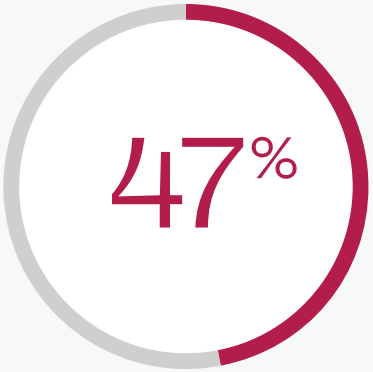
Por qué los códigos QR siguen siendo una de las principales amenazas para la seguridad y qué puede hacer al respecto

Códigos QR: Dónde empezaron y hacia dónde van

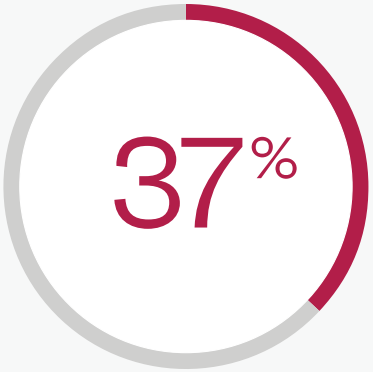
En 2020 registramos el creciente uso -y los potenciales riesgos de seguridad- de los códigos de respuesta rápida (QR). Aunque los códigos QR existen desde hace décadas, su uso se disparó durante la pandemia del COVID-19, cuando las transacciones sin contacto pasaron a ser la norma a nivel mundial. Cada vez más, los consumidores utilizan los códigos QR para acceder a sitios web, enviar pedidos y realizar pagos; por su parte, las autoridades gubernamentales los utilizan para facilitar la localización de contactos y el control de visitantes en los puestos de control fronterizos. Los códigos QR hicieron posible todos estos intercambios, sin dinero en efectivo y sin papel, cuando el mundo más lo necesitaba.

Avancemos hasta 2021: ¿qué ha cambiado? (si es que ha cambiado algo)

Sabemos que los códigos QR están más extendidos que nunca. Piense que las plataformas de redes sociales, como Facebook, Snapchat, Twitter, LinkedIn e Instagram, permiten a los usuarios seguir cuentas al instante con tan solo escanear un código QR. Por otra parte, los códigos QR son ya prácticamente omnipresentes en China, y en Corea del Sur y la India también han experimentado una rápida adopción. Las soluciones de pago con código QR se implantarán pronto en Ghana, Rusia y Sri Lanka, y a lo largo del próximo año se espera que más países habiliten esta tecnología.



de los encuestados sabía que un código QR puede abrir una URL, frente al 61 % de septiembre del 2020.



de los encuestados sabía que con un código QR sirve para descargar una aplicación, frente al 49 % de la encuesta anterior.

¿Cómo será la previsión de seguridad de los códigos QR en 2021?

Si nos atenemos alos resultados de nuestra encuesta, la previsión no es muy buena. Como señalamos en nuestro informe de 2020, las amenazas a la seguridad no residen en el propio código QR, sino en la falta de concienciación de los consumidores sobre las acciones que pueden realizar los códigos QR sin que el propio usuario lo sepa. Los arriesgados hábitos de los consumidores, unidos a la falta general de seguridad de "confianza cero" en los dispositivos móviles, no han mejorado el panorama de las amenazas móviles en los últimos meses.

Como resumen, nuestra encuesta de 2021 puso de manifiesto las siguientes tendencias:

- El uso de los códigos QR está aumentando, pero el conocimiento de lo que pueden hacer se queda muy atrás.
- Los casos de uso de los códigos QR se han ampliado, abarcando también los negocios personales, como las transacciones financieras y el acceso a la sanidad.
- Estas dos tendencias -la expansión del uso de los códigos QR y la falta de concienciación de los usuarios- pueden potencialmente poner, tanto a los consumidores como a las organizaciones, en un mayor riesgo de violación de datos.

Es un hecho que los códigos QR han llegado para quedarse, así que ¿cómo pueden los profesionales de la seguridad informática proteger a sus organizaciones contra las vulnerabilidades que esconden? El resto del informe analiza las tendencias globales de los códigos QR y ofrece información que las organizaciones pueden utilizar para fortalecer sus estrategias de seguridad en el futuro.

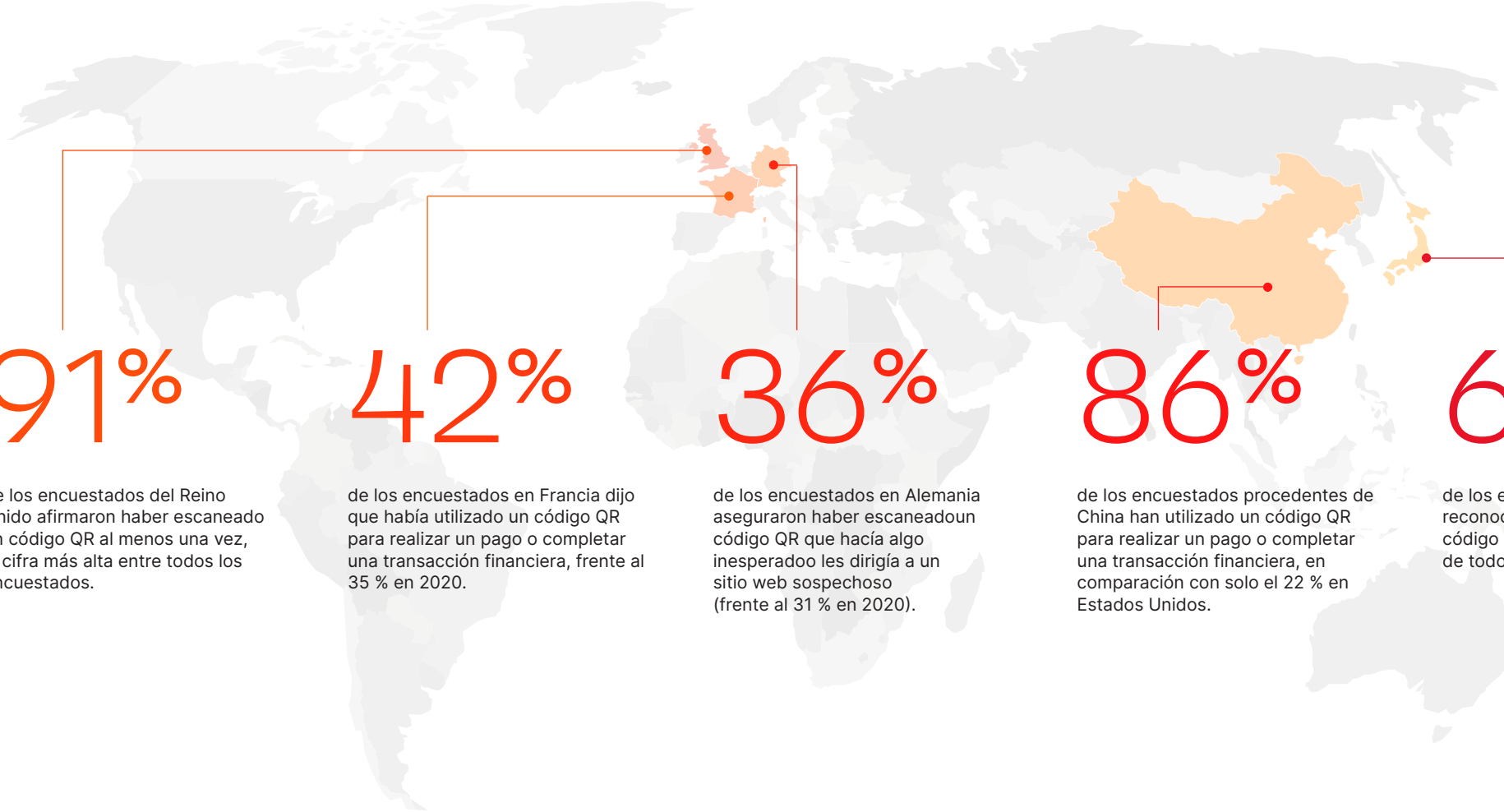
¿Sigue el mundo entusiasmado con los códigos QR?

Entre los países que estudiamos, descubrimos que la adopción de los códigos QR por parte de China superó ampliamente a la de todos los demás países. Por ejemplo, China ha adoptado rápidamente los códigos QR para todas las actividades, mientras que otros países los utilizan principalmente para agilizar las transacciones en restaurantes, bares y cafeterías. Resulta interesante que más del 40 % de los encuestados procedentes de China, afirmen haber escaneado un código QR en los últimos seis meses para asuntos financieros, como por ejemplo acceder a una cuenta bancaria, al extracto de una tarjeta de crédito o a un cajero automático. Curiosamente, solo un 7% de los encuestados en Estados Unidos declaró utilizar los códigos QR para realizar transacciones financieras.

Lo más llamativo de los resultados del estudio en este año, es que Japón -donde los códigos QR se inventaron hace décadas para agilizar el montaje de automóviles- ha sido más lento en la adopción de los códigos QR en comparación con otros países. De hecho, solo el 61% de los encuestados japoneses dijo haber escaneado alguna vez un código QR, el porcentaje más bajo de todos los países encuestados. Quizá lo más destacable sea que el uso de los códigos QR parece estar disminuyendo en Estados Unidos.

Menos de un tercio de los encuestados afirmó haber escaneado un código QR en la última semana, frente al 39% en 2020. El número de personas que reconoció haber escaneado un código QR en el último mes se redujo en 10 puntos porcentuales -de un 66% en 2020 a solo un 56% a principios de 2021.

Aunque los motivos que explican la tendencia a la baja en los Estados Unidos siguen sin estar claros, en general, la confianza de los consumidores en los códigos QR tiende a aumentar, lo que supone más oportunidades para que los ciberdelincuentes puedan explotar y hacer un uso indebido de esta tecnología.



91%

de los encuestados del Reino Unido afirmaron haber escaneado un código QR al menos una vez, la cifra más alta entre todos los encuestados.

42%

de los encuestados en Francia dijo que había utilizado un código QR para realizar un pago o completar una transacción financiera, frente al 35 % en 2020.

36%

de los encuestados en Alemania aseguraron haber escaneadoun código QR que hacía algo inesperadoo les dirigía a un sitio web sospechoso (frente al 31 % en 2020).

86%

de los encuestados procedentes de China han utilizado un código QR para realizar un pago o completar una transacción financiera, en comparación con solo el 22 % en Estados Unidos.

61%

de los encuestados japoneses reconoció haber escaneado un código QR, el porcentaje más bajo de todos los países encuestados.

¿El aumento de la confianza implica un mayor riesgo de los códigos QR?

Aunque nuestra encuesta encontró diferentes tasas de adopción en los distintos países, la confianza en los códigos QR aumentó de forma generalizada. En muchos casos, los consumidores expresaron una menor preocupación y sensibilización sobre los posibles riesgos de seguridad de los códigos QR. Por ejemplo, los encuestados de 2021 estaban menos preocupados por la privacidad (51 %) y las infracciones financieras (46 %) en comparación con 2020, cuando al 58 % les preocupaba la privacidad y más de la mitad (51 %) tenían preocupaciones financieras. Además, el conocimiento general de las acciones que pueden realizar los códigos QR, como por ejemplo abrir una URL, enviar un texto o revelar la ubicación del usuario, descendió en todas las categorías.

El hecho de que solo alrededor de la mitad (51 %) de los usuarios no tenga – o no sepa si tiene -, un software de seguridad instalado en sus dispositivos móviles, significa que las organizaciones de TI deben priorizar la seguridad contra los códigos QR maliciosos en 2021.

Por ello, no es de extrañar que cada vez más consumidores utilicen los códigos QR para sus asuntos personales sin pensar demasiado en la seguridad. De hecho, el 83 % de los encuestados afirmó haber utilizado un código QR para realizar un pago o completar una transacción financiera en el último año. De estos encuestados, el 54 % ha utilizado un código QR por un motivo financiero en los últimos tres meses. Este espectacular aumento podría deberse a una menor preocupación por la seguridad, así como a la normalización de los pagos sin contacto durante la pandemia.

Sin embargo, esta es la revelación verdaderamente preocupante para la seguridad: Aunque se ha registrado un uso decreciente generalizado de los códigos QR entre los consumidores, se siguen utilizando para acceder a información más sensible, como la información de las tarjetas de crédito, las cuentas bancarias y los registros sanitarios. Al mismo tiempo, los códigos QR realizan con mayor frecuencia acciones que el usuario no esperaba o, lo que es peor, le dirigen a sitios web maliciosos. Esto, sumado al hecho de que casi la mitad (51 %) de los usuarios no tienen - o no saben si tienen - un software de seguridad instalado en sus dispositivos móviles, significa que las organizaciones de TI deben priorizar la seguridad contra los códigos QR maliciosos en el 2021.

83%

de los encuestados afirmó haber utilizado un código QR para realizar un pago o una transacción financiera en el último año. De estos encuestados, el 54 % utilizó un código QR por un motivo financiero en los últimos tres meses.

47%

de los encuestados sabía que un código QR es capaz de abrir una URL, frente al 61 % de 2020, lo que supone un descenso de 14 puntos porcentuales.

37%

de los encuestados sabía que un código QR podía descargar una aplicación, lo que supone un descenso de casi 12 puntos porcentuales con respecto a 2020.

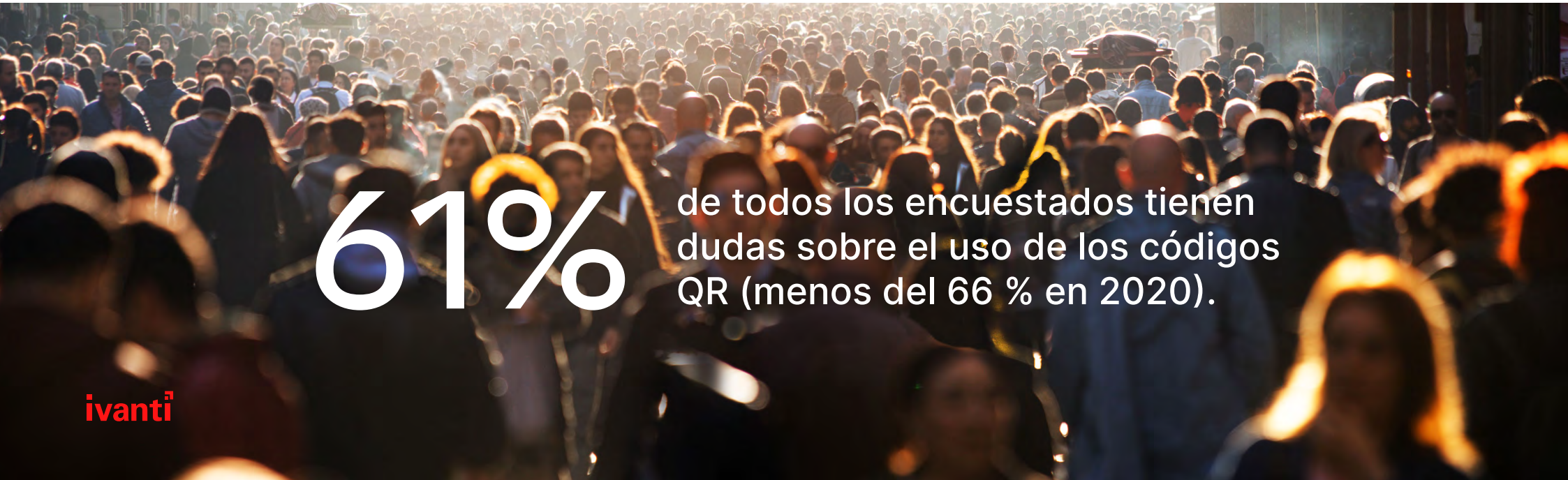
¿Cómo ha cambiado el panorama de las amenazas móviles?

Como refleja nuestra investigación, menos de la mitad de los consumidores de todo el mundo tienen seguridad móvil en sus dispositivos. Los ciberdelincuentes también son conscientes de este hecho, por lo que han cambiado sus tácticas para dirigirse a los usuarios de móviles, que generalmente son menos seguros y están más distraídos que los usuarios de equipos corporativos. El uso de códigos QR para realizar ataques maliciosos en dispositivos móviles quedó documentado ya en 2013, cuando quedó claro que los hackers vinculaban los códigos QR a sitios web incrustados con malware. El sitio web malicioso infectaba al dispositivo con un troyano, que luego desencadenaba ataques de vigilancia y exfiltración de datos y enviaba esta información a los servidores del hacker.

El panorama no ha cambiado mucho desde entonces, exceptuando el hecho de que los códigos QR se utilizan mucho más en 2021 que en 2013, y para más transacciones. Esto, unido al desconocimiento general sobre el funcionamiento de los códigos QR por parte de los consumidores, los convierte en una herramienta increíblemente potente para los hackers.

Hoy en día, los consumidores pueden escanear involuntariamente códigos QR fraudulentos, que les llevan a un sitio web de apariencia legítima que pide a los usuarios que proporcionen datos como el nombre de usuario y la contraseña, la información de la tarjeta de crédito y el nombre de la empresa, entre otros. El ciberdelincuente utiliza entonces esta información para acceder a las cuentas del usuario o a las aplicaciones y datos corporativos que pueda haber en el dispositivo. Y, al igual que los troyanos del pasado, en 2021 los códigos QR pueden seguir utilizándose para descargar software malicioso en un dispositivo móvil sin que el usuario lo sepa.

Aunque las técnicas han cambiado y siguen evolucionando, el objetivo es el mismo: acceder a la información de valor. Por ello, es más importante que nunca disponer de una base de seguridad móvil que pueda proteger contra estas amenazas en continua evolución.



La protección contra las amenazas requiere seguridad móvil y educación de los usuarios

No es de extrañar que los hackers sigan utilizando los códigos QR para acceder a los dispositivos móviles, las aplicaciones y los datos. Esto se debe en gran medida a que los códigos QR son baratos y fáciles de generar y explotar. Una combinación de educación del consumidor, una buena higiene de seguridad y una sólida plataforma de seguridad móvil puede ayudar a minimizar -o incluso eliminar- por completo estos riesgos.

Qué pueden hacer los usuarios

- Nunca confíe en los correos electrónicos de remitentes desconocidos (lo cual es una buena práctica de seguridad, en general).
- Trate los códigos QR desconocidos igual que las URL desconocidas, que es esencialmente lo que son.
- Asegúrese de que el código QR es el original y no se ha pegado con otro si se encuentra en un lugar físico, como el expositor de una tienda.
- Utilice un software de escáner QR para ver la URL antes de hacer clic en ella.

Qué pueden hacer las empresas

Como se ha mencionado anteriormente, los usuarios no suelen tener ni idea de si existe algún tipo de seguridad en sus dispositivos móviles. Para ser honestos, así es como debería ser. Los empleados remotos deben poder seguir siendo productivos sin tener que actualizar constantemente el software de seguridad o introducir contraseñas para acceder a las aplicaciones y a los datos de la empresa.

La seguridad móvil de "confianza cero" que valida cada dispositivo, usuario, aplicación, URL, red y nube, es fundamental para la protección contra el phishing u otros fraudes por internet que aprovechan los códigos QR para eludir el software antivirus tradicional. En concreto, las organizaciones necesitan una plataforma completa de gestión y seguridad de dispositivos móviles que pueda descubrir, gestionar y proteger todos los dispositivos que acceden a los recursos empresariales.

La capacidad de ver y proteger cada dispositivo en el Everywhere Workplace (lugar de trabajo "en todas partes"), permite defenderse de los delitos informáticos, así como de las amenazas a los dispositivos, las aplicaciones y la red, incluso cuando los dispositivos no están conectados a la red. Además, al ampliar el uso de la autenticación multifactor, las empresas pueden también eliminar las contraseñas, una de las principales causas de las violaciones de datos relacionadas con el delito informático.

ivanti

ivanti.com
1 800 982 2130
sales@ivanti.com

I. [Report overview]
II. In September 2020, MobileIron (acquired by Ivanti in December 2020) conducted an ambitious survey of nearly 4,500 consumers across the U.S., U.K., Germany, Netherlands, France and Spain. (The results of that report can be found here.) At the start of 2021, Ivanti expanded the survey to include consumers in China and Japan, which replaced Spain and the Netherlands in the survey. The current study offers a broader picture of how QR codes are being used beyond the U.S. and western Europe — giving security professionals more insight into global QR code trends.