**Madrid, 10 de noviembre de 2021**

**QRishing: cuando los códigos QR son tanto o más peligrosos que los emails y links maliciosos**

**En un mundo cada vez más digital, el arraigo en la sociedad de que hay que evitar los emails de origen desconocido y los links usurpadores de identidad está cada vez más extendido, lo que da paso a la siguiente herramienta que hackers y piratas informáticos utilizan con cada vez mayor asiduidad y que, claramente, cuenta con que la sociedad casi 100% digital de hoy en día aún no está preparada mediática y psicológicamente para evitarlos: el QRishing o los códigos QR maliciosos**

La sociedad digital, donde todo funciona a través de “La Nube”, es más segura y práctica que la sociedad del papel o el plástico, ya que es más fácil perder un billete o un DNI que la información que uno puede rescatar en cualquier móvil, Tablet u ordenador. Pero estas herramientas también tienen un peligro que no se ve, pero que está ahí y que, a menudo, la gente se da cuenta cuando su Instagram ya no es el suyo, cuando sus claves del banco han sido modificadas o, peor aún, cuando su identidad digital o su dinero han pasado, sin comerlo ni beberlo, a manos equivocadas.

Según [SICPA](https://www.sicpa.com/), líder mundial en seguridad de la identidad digital y en sistemas informáticos y físicos antifraude, actualmente existe una herramienta muy común entre los hackers y ladrones informáticos conocida como “phishing” que, básicamente gracias a ella roban o amenazan a los usuarios que se fían de un anuncio o un concurso recibido en su email o bandeja de SMS del móvil de una manera muy rápida y “limpia”: se pincha en el link en el que se asegura que se ha ganado un concurso de dos millones de euros e, inmediatamente, se le roba al “pobre ingenuo” todo tipo de información sensible.

Este sistema ya está muy extendido, y la gran mayoría de la sociedad sabe cómo evitarlos (directamente dar a la tecla “suprimir” cuando se recibe este tipo de comunicación digital, sin abrirla antes, no visitar algunas páginas de dudosa identidad…), pero esto también ha supuesto que los piratas digitales cambien su modus operandi. De hecho, ya antes de la pandemia de la COVID-19, en el año 2012, [la Carnegie Mellon University (Pittsburgh, Pensilvania, EEUU) realizó un estudio de lo que ya denominó como **QRishing,**](https://www.cylab.cmu.edu/_files/pdfs/tech_reports/CMUCyLab12022.pdf) o la susceptibilidad de los usuarios de teléfonos inteligentes a los ataques de “phishing” vía códigos QR.

En su estudio, *observaron que el 85% de las personas que escanearon un código QR visitaron posteriormente la URL asociada. Y estimaban que este porcentaje podría llegar a casi el 100%, ya que la tendencia del usuario cada vez mayor es la de no plantearse que haya algo malicioso detrás de un algoritmo encriptado.*

Pero ¿qué pasa cuando se lee un QR? La acción se asemeja a cuando se pincha directamente un link de Internet, se está pinchando en un enlace que ni siquiera se puede ver a simple vista, con lo que la probabilidad de caer en las redes de una web maliciosa aumenta exponencialmente, sobre todo si se compara con el caso de un email, un SMS o un WhatsApp “pirata”, en los que sí se puede identificar más fácilmente a dónde quieren redirigir si se pincha en ellos. Básicamente, la ausencia de información gráfica fomenta que la gente lea QRs.

Y estos QR maliciosos no solo sirven para robar identidades o información sensible, sino también para falsificar o recrear una realidad casi paralela y, prácticamente siempre, ilegal. Recientemente se han visto Data-Matrix (un tipo de código QR) de Pasaportes COVID falsificados con identidades como Adolf Hitler, Mickey Mouse y Bob Esponja que, para más inri, han sido validados y reconocidos por las apps gubernamentales.

Por ello, compañías como [SICPA](https://www.sicpa.com/offices/spain-alcala-de-henares-madrid), líder mundial en seguridad de la identidad digital y en sistemas informáticos y físicos antifraude, que trabaja esencialmente con Gobiernos y Comunidades Autónomas, velan por que la sociedad digital siga siendo más segura y práctica que la antigua del papel y del plástico.

En este sentido[, SICPA, que cuenta con oficinas y una planta de I+D+i con más de 150 trabajadores en Madrid (España)](https://www.sicpa.com/offices/spain-alcala-de-henares-madrid) vio que, a medida que el potencial de la tecnología digital comenzó a cambiar de un modo evidente las necesidades de seguridad a través de productos como blockchain, tomó la decisión estratégica de investigar e idear aplicaciones específicas para ofrecer seguridad y confianza en este nuevo universo. De este modo, creó áreas estratégicas de negocio centradas exclusivamente en salvaguardar la integridad digital, con el apoyo de un laboratorio de aplicaciones digitales y la iniciativa de la moneda digital del Banco Central (CDB), que han dado lugar a innovadores productos como [la plataforma Certus®, que incluye la certificación de salud y vacunas a través de myHealth Pass](https://www.sicpa.com/MyHealthPass), así como otras aplicaciones creadas para hacer frente a nuevos desafíos, como la protección de los registros de tierras, la integridad electoral, los diplomas o la identidad digital de los trabajadores de una empresa concreta, entre otros.

Certus® es una solución digital novedosa que permite a los emisores de documentos de valor, como instituciones educativas, organismos gubernamentales y notarios, asegurar sus certificados con una combinación de sellos digitales con códigos QR a prueba de manipulaciones. El resultado es una marca de código QR que es imposible de manipular o falsificar y asegura tanto los certificados en papel como los digitales, permitiendo una verificación independiente y universal y salvaguardando el valor de los documentos de los titulares y la reputación de las autoridades emisoras.

De esta manera, empresas como SICPA velan por la seguridad de la sociedad digital hasta que ésta se conciencie de la peligrosidad del “QRishing” de la misma manera que lo ha hecho con el “Phishing”, para prevenir que el ciudadano cotidiano pase a ser el agente intermedio involuntario de un ataque por parte de ciberdelincuentes que fijen su objetivo en el individuo mismo o en las empresas e instituciones.

[**Acerca de SICPA**](https://www.sicpa.com/)

Fundada en 1927, SICPA es una empresa internacional con 3.000 empleados de más de 50 nacionalidades, y con sedes, instalaciones de producción y centros de excelencia en todos los continentes. Fundada en Lausana (Suiza) por Maurice Amon, la empresa 100% familiar comenzó suministrando su producto original, una grasa especial para ordeñar vacas, a la industria agrícola y alimentaria del país alpino. Desde entonces, SICPA no ha dejado de innovar con sus sistemas de monitorización de la producción para combatir con éxito la falsificación, el comercio ilícito y la evasión fiscal, con productos cada vez más sofisticados, como SICPATRACE®, un sistema seguro de identificación de productos, trazabilidad y conciliación fiscal; SPARK®, la primera tinta dinámica de cambio de color aplicada a los billetes; la tecnología de tinta legible por máquina NEOMAG®; SPARK® Live, que creó unas nuevas dinámicas de seguridad óptica y que actualmente se utiliza en más de 40 países; un exclusivo sistema de marcado molecular para luchar contra los fraudes de combustible; o Certus®, que incluye la certificación inviolable de cualquier identificación digital.

En España, SICPA cuenta con un área de desarrollo de soluciones en Alcalá de Henares (Madrid), que cuenta actualmente con nueve equipos de desarrollo y uno de soporte, compuestos por más de 130 personas, con un 21% de mujeres y 14 nacionalidades diferentes, así como por unas oficinas centrales con más de 100 personas en plena calle Velázquez (Madrid).

**Para más información:**

**Eugenia Marcos**

emarcos@vopress.es

Tel. 670 70 06 54/ 915 343 090

**Hugo Fraile**

hfraile@vopress.es

Tel. 617 155 466 / 915 343 090

**Arancha Yagüe**

ayague@noho.es

Tel. 617 833 233 / 915 343 090