Edición No. 10 – septiembre 2021

Seguridad Informática en el sector Salud

¡Porque la seguridad es de todos!

CARTAS QR NUEVA AMENAZA PARA LA PRIVACIDAD

Debido a la pandemia y al distanciamiento social, las **cartas QR** se han convertido en una constante en las cafeterías, bares y restaurantes ofreciendo una alternativa de **"transacción sin contacto"** diferente a tener las cartas impresas, aunque el código bidi ya estaba presente antes de la crisis sanitaria, este ha contribuido a extender su uso más allá de lo imaginado.

Muchos usuarios ven con buenos ojos esta iniciativa y se han acostumbrado a su uso cada vez más popular, y a consecuencia del éxito de las cartas QR, a corto plazo veremos como se expande en otros entornos, como consecuencia de la familiaridad y facilidad que se ha adquirido en estos tiempos.

Pero, **¡CUIDADO!,** tras la tecnología QR se puede esconder un sofisticado sistema de rastreo que analiza el comportamiento de los clientes, recopilando en algunos casos, datos sensibles y protegidos, como los datos personales, el historial de pedidos, el correo electrónico y el número de móvil.

Según alerta **The New York Times,** ya hay sistemas que recopilan datos sobre las consultas de las cartas en QR que, con algunos datos adicionales, permiten rastrear a los clientes y pueden llegar a ser utilizados por los responsables de marketing de otras industrias, elaborando publicidad segmentada. No quiere decir esto que se esté desmeritando el uso de las cartas QR, estas son ideales para la no transmisión del coronavirus y otro tipo de enfermedades adquiridas por contacto, pero si es una señal más de que los responsables de los navegadores deben tratar que sean más seguros y poder mantener nuestra privacidad a salvo. La actual ***política de privacidad*** no contempla nada concreto sobre esta circunstancia, facilitando así que los restaurantes puedan utilizar los datos a su antojo o incluso compartirlos y venderlos a un tercero.

Pero no todos los QR son iguales. Lo más frecuente es que su uso simplemente nos envíe a una web o un archivo donde vamos a encontrar la carta del restaurante. Pero en otros casos, se están implementando complejos sistemas de rastreo digital, capaces de obtener todo tipo de datos sensibles en el momento en el que leemos el QR de la carta.

***Fuente*: http://www.techno-partners.com**

Edición No. 10 – septiembre 2021

Seguridad Informática en el sector Salud

¡Porque la seguridad es de todos!

BUENAS PRACTICAS DE SEGURIDAD

Debemos proteger nuestro **PUESTO DE TRABAJO** y mantener la mesa "limpia" de papeles que contengan información sensible.

Es recomendable establecer en tu **DISPOSITIVO MÓVIL** una clave de acceso y la opción de bloqueo automático.

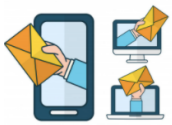
No hagas uso de **EQUIPOS NO CORPORATIVOS**. Si es necesario, no manejes información corporativa en este tipo de equipos.

Evita las **FUGAS DE INFORMACIÓN**. No mantengamos conversaciones confidenciales en lugares donde puedan ser escuchadas por terceros.

LAS CONTRASEÑAS deben de ser secretas y únicas, no debemos anotarlas, compartirlas o reutilizarlas.

Se debe realizar una **NAVEGACIÓN SEGURA** y evitar acceder a páginas web no confiables.

https://



Utiliza el **CORREO ELECTRÓNICO** de forma segura, elimina e informa a tu departamento de informática todo correo sospechoso que recibas.

Protege **LA INFORMACIÓN** y realiza copias de seguridad de la información sensible que solo esté en nuestro equipo.

Cuando **VIAJES**, no envies información sensible a través de redes WIFI no confiables.

TODOS SOMOS SEGURIDAD. Debemos avisar al área de sistemas de la institución si detectamos cualquier actividad sospechosa.

Fuente: ***INCIBE y la Oficina de Seguridad del Internauta (OSI).***