Asociación Bancaria Costarricense

Bancos recomiendan precaución al utilizar códigos QR

- *Uso inadecuado puede llevar al cliente a una página falsa donde capturan su información confidencial.*
- *Bancos los utilizan con fines informativos y en algunos casos como medios de pago, pero aplicando todas las medidas de seguridad necesarias.*

Marzo, 2022. En la era tecnológica, en la que estamos inmersos, cada vez contamos con más recursos para agilizar determinados procesos en bancos, comercios y empresas de todo tipo; los códigos QR son una de esas herramientas que se han popularizado, pero la Asociación Bancaria Costarricense (ABC) hace un llamado para utilizarlos con precaución y responsablemente.

En el país algunas entidades financieras los utilizan únicamente con fines informativos y en otras como medios de pago, pero siempre aplicando todas las medidas de seguridad necesarias para resguardar la información de los clientes.

Al escanear un código QR, este lo que hace es que lleva a la persona a una página web, donde puede ver determinada información, por ejemplo: el menú en restaurantes o detalles sobre un determinado producto o servicio. Sin embargo, su uso implica tomar las precauciones necesarias para no ser víctima de una estafa, ya que los grupos criminales también los utilizan.

"Así como podemos descargar fácilmente esta información, los ciber delincuentes también utilizan los códigos QR para hacer que las personas descarguen contenido malicioso y robar información de sus dispositivos o los llevan a páginas falsas para robar usuarios y contraseñas, para luego acceder a sus cuentas y sustraer el dinero", manifestó Raúl Rivera, Asesor en ciberseguridad de la ABC.

Tipos de ataque a códigos QR

- **QRishing**: Llevan a la persona a una página web falsa donde capturan la información confidencial: usuarios, contraseñas y códigos de seguridad.

- **Descarga de código malicioso**: Redireccionan a una página web que descarga un código malicioso en el dispositivo que puede infectarlo con un virus: Troyano, Spyware, Botnet o Cryptomining.

- **QRLjacking**: Una vez que la persona ingresa a un sitio web o red social secuestran la sesión engañándolo para ingresar mediante el uso de un código QR, similar a lo que utilizar WhatsApp para ingresar al WhatsApp Web.

Recomendaciones para el uso seguro de códigos QR

- **A nivel personal:**
    - **Utilizar un escaneador seguro de códigos QR**. Generalmente se utiliza la cámara del teléfono o tableta, lo que aumenta el riesgo.
        - Kaspersky (Android, iOS) - Descargar Lector Seguro de Códigos QR | Kaspersky
        - TrendMicro (Android) – Descargar el Lector Seguro de Códigos QR | Trend Micro

    - **Deshabilitar que las direcciones URL abran de forma automática** después de escanear el código. Esto le permitirá revisar si el URL tiene algún elemento o comportamiento malicioso.

    - **Verificar si el URL es confiable**, para ello solamente debe copiar el URL escaneado antes de abrirlo, visitar la página www.virustotal.com, seleccionar donde dice URL, pegarlo en el campo que allí aparece y presionar ENTER.

- **A nivel comercial:**

    - **Los establecimientos que utilizan códigos QR deben comprobar periódicamente que estos no hayan sido cambiados**. Los ciberdelincuentes alteran los códigos para defraudar a los clientes.

    - **Utilizar un generador confiable o seguro de códigos QR**. Algunos sitios web que generan códigos QR de forma gratuita, pueden inyectar acciones maliciosas o descargar código malicioso, además de las acciones que se configuren normalmente para realizar.

"Los bancos realizan grandes esfuerzos para velar por la seguridad de sus clientes y resguardar su dinero, pero es vital que las personas desconfíen y nunca compartan su información sensible, como usuarios, claves o contraseñas, las entidades financieras nunca pedirán esos datos", concluyó Raúl Rivera, Asesor de ciberseguridad de la Asociación Bancaria Costarricense.

Para mayor información o concertar una entrevista, no dude en contactarme.

Fanny Alvarado Q.
Imagen y Comunicación Creativa
2283 7101 ext. 108 / 8379-9137
falvarado@iccasesores.com