

## Asociación Bancaria Costarricense alerta sobre timos que se utilizan en las últimas semanas del año

- *El falso funcionario municipal y el código QR para capturar datos sensibles o descargar malware son algunas de las técnicas de los delincuentes.*
- *ABC también recuerda la importancia de desligar las cuentas de SINPE Móvil del número de teléfono, cuando se hace cambio de línea*

**Diciembre, 2024.** La Asociación Bancaria Costarricense (ABC) hace un llamado para que las personas se protejan contra los métodos de fraude electrónico utilizados por la delincuencia en la época de fin de año.

La ABC se mantiene en contacto con las autoridades del Organismo de Investigación Judicial (OIJ) para detectar las estrategias del hampa, advertir a los consumidores financieros y evitar que caigan en los engaños.

“El mensaje principal es que siempre debemos mantener la guardia en alto y no hacer caso de llamadas telefónicas, mensajes de texto o correos electrónicos que provengan de fuentes no verificables. Es muy importante redoblar esa actitud de seguridad en diciembre, cuando hay más dinero circulando y aumenta el comercio de todo tipo”, afirmó Raúl Rivera, Asesor de Seguridad de la ABC.

Estos son algunos de los métodos de fraude electrónico que aumentaron en las últimas semanas, de acuerdo con el OIJ y la ABC:

### Impuestos municipales

Como en diciembre se acostumbra a pagar los impuestos de las casas, cobra fuerza el timo del falso empleado municipal.

En estos casos, el delincuente contacta a la potencial víctima para insistir en la necesidad de pago e inclusive ofrecerle algún descuento si cancela de inmediato, para lo cual lo guiará a través de un proceso cuyo objetivo es capturar su información bancaria.

El ABC recuerda no confiar en cualquier llamada donde no pueda confirmarse la identidad del interlocutor, por lo que es importante cortar esa interacción y comunicarse de forma directa con la institución relacionada para confirmar la situación.

### Escaneo de códigos QR

En varios países de Latinoamérica algunas personas reportan haber encontrado un código QR pegado a su vehículo, con el aviso de una infracción de tránsito por estacionarse mal, donde el QR supuestamente permite ver en detalle el parte, pero en realidad lleva a una página falsa donde tomarán los datos personales y bancarios de la víctima. También es muy común ir a un restaurante o comercio y encontrarse este tipo de códigos QR para realizar sus pagos; sin embargo, puede ocurrir que los delincuentes peguen una calcomanía encima para llevarlos a páginas de pago falsas.

La ABC recomienda no escanear ningún código QR que aparezca de forma repentina, sin posibilidad de comprobar su procedencia. Siempre verifique con la contraparte o realice sus pagos a través de las plataformas oficiales disponibles.

### Cuentas asociadas a SINPE Móvil

El OIJ registra denuncias de usuarios de SINPE Móvil que cambiaron de línea telefónica, pero por un descuido dejaron la cuenta ligada al número telefónico anterior y sufrieron la pérdida de su dinero.



La ABC recuerda estar muy atentos a desactivar el SINPE Móvil en caso de un cambio de línea, ya sea prepago o postpago, y después volver a afiliarse con el nuevo número.

### **Falsa venta o compra de productos**

También para esta época aumentan las ventas de productos por redes sociales y otros medios digitales, donde solicitan depositar el dinero sin entregar el producto. Por otra parte, si la potencial víctima está vendiendo algún producto, los delincuentes envían fotografías de pago falsas, y generalmente mandan de inmediato a un tercero a recoger el objeto antes de que el vendedor vea los fondos reflejados en su cuenta.

La ABC recuerda siempre validar y verificar la acreditación de un pago y, en caso de dudas, confirmar con la institución financiera de forma directa y nunca a través de su interlocutor.

Finalmente, Raúl Rivera, Asesor de Seguridad de la ABC, señaló que para completar transacciones financieras es mejor evitar las redes WiFi públicas, pues poseen menos garantías y podrían permitir a los delincuentes capturar la información.

Asdemás, si utiliza computadoras portátiles, celulares o tabletas, debe instalar un antivirus para protegerlos de programas maliciosos o sitios ya identificados como fraudulentos, pues en el fondo todos esos dispositivos son computadoras