- *Delincuentes usan timos como el supuesto cobro indebido del impuesto de renta y falsas exoneraciones por la emergencia del COVID-19, para conseguir información y robar dinero.*
- *Bancos nunca piden información sensible, como claves o token, por teléfono ni correo.*

Mayo, 2020. La Asociación Bancaria Costarricense (ABC), que agrupa los 14 bancos públicos y privados del país, hace un llamado a la ciudadanía para que esté alerta ante los intentos de estafas y eviten dar información secreta de sus cuentas a los delincuentes, pues los pueden dejar sin su dinero.

"Los bancos hacen todos los esfuerzos necesarios para proteger el dinero de los costarricenses, pero es imprescindible que los clientes entiendan que no debe brindar información clave a nadie. Los propietarios de cuentas deben informarse por las fuentes oficiales para no caer en engaños y timos de bandas organizadas", indicó María Isabel Cortés, Directora Ejecutiva de la ABC.

Ante la emergencia nacional por el COVID-19, las visitas a las sucursales digitales se incrementaron, así como el uso de los servicios on line y las aplicaciones para celulares. Según datos del Banco Central de Costa Rica (BCCR), en marzo se suscribieron 70 mil personas al servicio de Sinpe Móvil, lográndose un total de 1.700.000 usuarios y se realizaron un 1.272.000 de transferencias.

En las últimas semanas los delincuentes están utilizando dos timos:

1. Al llamar le indican a la víctima **que son del Ministerio de Hacienda**, que la entidad incurrió en un error al realizar el débito del impuesto de renta y que le han estado cobrando más, por lo que es necesario que llene un registro de exoneración para que le realicen el reintegro del dinero. El supuesto funcionario le dice a la víctima que la entidad no pide información sensible por teléfono y se ofrecen a guiarlo en la página de la institución para realizar el trámite.
2. **Dicen ser de la Dirección General de Tributación Directa** y que realizarán una exoneración del 50% en el pago de servicios públicos, supuestamente por una orden presidencial, ante la emergencia por el COVID-19, pero que para ello es necesario llenar un formulario y una autorización con firma digital. Nuevamente se ofrecen a acompañarlo para realizar el proceso.

En ambos casos, logran engañar a la víctima hasta que esta da acceso remoto a su computadora y también brinda claves o token para acceder a los servicios bancarios. Una vez que el estafador tiene esta información, solamente entretiene al cliente mientras saca el dinero de la cuenta y de esa manera impide que la víctima atienda la llamada del banco. Ante cualquier sospecha, los buscan siempre alertar al cliente de movimientos sospechosos en sus cuentas.

Para la ABC es importante que los clientes se mantengan informados por las fuentes oficiales, para que puedan identificar desde el inicio que lo que les proponen es falso. Además, deben tener claro que ninguna institución les pedirá claves de sus cuentas o acceso remoto a su computadora.

También es importante tomar medidas de seguridad al utilizar las páginas web de las entidades bancarias, por ejemplo:

- No utilizar buscadores, ya que lo pueden llevar a páginas falsas. Se debe acceder únicamente digitando en la barra de navegación la dirección completa del banco.
- Tener cuidado con las compras por internet.
- Acceder siempre desde computadoras seguras y privadas, evitando usar contraseñas en máquinas públicas.

Si el cliente sospecha o ya fue víctima de una estafa, debe comunicarse con su banco, donde le informarán sobre el procedimiento a seguir. También debe interponer la denuncia correspondiente ante el Organismo de Investigación Judicial (OIJ).

"La ABC reitera que ninguna entidad bancaria solicita a los clientes información por correo electrónico o llamadas telefónicas, mucho menos claves de seguridad, por lo que deben estar alerta y entender que, si alguien se las solicita, aunque se identifique como empleado bancario o de una institución pública, se trata de una estafa", concluyó María Isabel Cortés, Directora Ejecutiva de la ABC.