Asociación Bancaria Costarricense

Expertos de la ABC insisten a la población para que esté alerta ante posibles estafas al iniciar el pago del aguinaldo

- *Delincuentes intentan obtener información para el acceso a cuentas bancarias por medio de correos, llamadas con suplantación de números de entidades bancarias, mensajes por WhatsApp y redes sociales.*
- *Bancos reforzarán operativos de seguridad en sucursales y cajeros automáticos.*

Noviembre, 2021. A pocas semanas para que miles de personas reciban el pago de su aguinaldo, la Asociación Bancaria Costarricense (ABC) reitera el llamado a la ciudadanía para que esté muy alerta ante posibles intentos de estafa y evite dar cualquier información personal de sus cuentas bancarias.

Los grupos criminales se valen del exceso de confianza para obtener datos que luego les permiten acceder a las cuentas bancarias de las víctimas y sustraer su dinero.

"Para obtener acceso a una cuenta bancaria necesariamente los delincuentes requieren de cierta información de su víctima, por eso intentarán contactarla por correo electrónico, por WhatsApp, redes sociales o incluso una llamada telefónica, muchas veces suplantando el número de alguna entidad bancaria, con tal de conseguir los datos de autenticación para ingresar a la cuenta. La población debe tener claro que cualquier solicitud de este tipo se trata de una estafa y debe cortar la comunicación de inmediato", manifestó Raúl Rivera, de la comisión de ciberseguridad de la ABC.

Los bancos nunca pedirán por teléfono, correo o mensaje, información sensible, como claves, ID o métodos de autenticación, como token, bingo card y clave dinámica.

Según Rivera los delincuentes también contactan a las víctimas haciéndose pasar por familiares o amigos que requieren alguna ayuda económica o en el caso de personas que tienen algo a la venta, dicen ser un posible comprador y aducen problemas para realizar el pago, para incluir a una tercera persona en la llamada, quien resulta ser un falso funcionario bancario.

Los principales tipos de ataque:

- "Ingeniería social (por correo, teléfono, mensajes o redes sociales) la mejor medicina para esto es no ser impulsivo y confirmar la fuente o remitente.
- Lo segundo es la suplantación de identidad. Es preciso verificar que se está en el sitio oficial de la entidad bancaria, además de contar con prácticas importantes como: contar con contraseñas robustas, no repetirlas en más de un sitio, cambiarlas periódicamente y acompañarlas de otros mecanismos de seguridad complementarios.
- El robo de datos, para ello es importante contar con antivirus y antimalware, así como buenas prácticas de seguridad para configurar de forma segura los dispositivos y privacidad de nuestros datos" indicó el experto.

Otras recomendaciones básicas son:

- No ver la ciberseguridad como un tema de alguien más.
- No dejarse presionar, hay que detenerte, pensar y actuar.
- La privacidad de los datos es muy importante, ¡no los facilite!
- Agregar contraseñas robustas y un doble factor de autenticación.
- No caiga o reenvíe noticas, correos o mensajes sin validar.
- Proteja todos sus dispositivos y no utilice programas piratas.
- Todo programa o dispositivo tiene guías de seguridad, ¡revíselas!

Refuerzo de operativos de seguridad

El asesor en temas de seguridad bancaria de la ABC, Rodney Jiménez explicó que trabajan desde ya en reforzar las medidas de seguridad para prevenir cualquier incidente en las distintas sucursales, pero también es importante que los clientes extremen los cuidados y sean muy precavidos con el manejo del dinero.

Dentro de los aspectos más importantes a considerar, por parte de los usuarios bancarios, es no dejar que los adultos mayores lleguen a retirar el dinero solos, pues son las víctimas que con mayor facilidad atacan los delincuentes que se dedican al marcaje o a cometer robos en las afueras de los bancos y los cajeros automáticos.

Seguridad en los cajeros automáticos

- Evite realizar el retiro de sumas altas de dinero en cajeros automáticos.
- Procure no visitar cajeros en altas horas de la noche.
- No le facilite a ninguna persona su pin de cajero, si tiene problemas visite una sucursal.
- Verifique que el cajero automático no presente ningún tipo de alteración, que ponga en riesgo su información.

"Cada año, las entidades bancarias realizan un monitoreo constante en las sucursales y cajeros automáticos ubicados en zonas de incidencia delictiva, de manera que ante cualquier eventualidad se pueda dar respuesta en el menor tiempo posible, como apoyo a los dispositivos de seguridad que se empezarán a implementar con los operativos del aguinaldo seguro", destacó Jiménez de la ABC.

Los bancos públicos y privados, afiliados a la Asociación Bancaria Costarricense han realizado importantes esfuerzos para reforzar la seguridad tanto en sucursales como en sus plataformas digitales, pero es preciso que los clientes también tomen en consideración todas las recomendaciones y las apliquen, de manera que no sean presa fácil de los delincuentes.

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