MEDIDAS DE SEGURIDAD BÁSICAS.

SSPC/ABR/2016

CON LA FINALIDAD DE DAR A CONOCER A LA POBLACIÓN EN GENERAL MEDIDAS BÁSICAS DE SEGURIDAD PARA EL USO DE TARJETAS BANCARIAS ASÍ COMO ASISTIR A SUCURSALES BANCARIAS Y UTILIZAR CAJEROS AUTOMÁTICOS, SE HACE DE SU CONOCIMIENTO LAS SIGUIENTES RECOMENDACIONES:

USO DE TARJETAS DE CRÉDITO Y/O DEBITO
"CUIDA TU CLAVE O NIP".

- Jamás revele a su número de clave (NIP), es información confidencial.
- Cuando realice retiro de efectivo en cajeros automáticos cubra todo el teclado al digitar su clave (NIP).
- No escriba o grabe en su celular o en papeles dentro su cartera el NIP.
- Cambie su NIP frecuentemente, al menos 2 veces al año.
- No asigne la misma contraseña o NIP a diferentes productos como Ahorros, Cuenta Corriente, Tarjeta de Crédito, Tarjeta de Débito, entre otros.
- Al realizar algún pago con su tarjeta bancaria no la pierda de vista, preferentemente solicite que lleven la Terminal Punto de Venta (TPV) hasta usted; por ningún motivo entregue su tarjeta a personas extrañas.
- No permita que deslicen su tarjeta en dispositivos diferentes a TPV o en cajeros automáticos.
- Cuando sea declinada su transacción solicite que le entreguen el boucher de rechazo.
- Siempre verifique el monto (cantidad a pagar) del boucher que firme.
- Cuando le entreguen una tarjeta bancaria nueva, fírmela inmediatamente e intente memorizar el número, le será benéfico al solicitar la cancelación o bloqueo por robo o extravío.
- Guarde en su celular y/o agenda los teléfonos de contacto que aparecen al reverso de su tarjeta para cualquier emergencia.

MEDIDAS DE SEGURIDAD PARA TRANSACCIONES POR INTERNET Y EVITAR ROBO DE IDENTIDAD

- Siempre haga sus transacciones bancarias en equipos de uso personal; no use cafés Internet, salas de sistemas u otros sitios públicos.
- Siempre que ingrese a una página para realizar transacciones sobre su cuenta, verifique que la dirección electrónica presentada en la parte superior de la pantalla sea https:// en lugar de la habitual http:// y que el navegador muestre el símbolo del candado cerrado en la parte inferior de la misma.
- Nunca ingrese usando un link que aparezca escrito en un correo electrónico, aunque provenga de alguien conocido.
- No crea en aquellos mensajes de correo que le sugieren entrar a su cuenta o dar información. Esto se conoce como 'phishing', una práctica ilegal en la que los delincuentes montan páginas web similares a las de la entidad bancaria para allí robarle sus claves y luego desocuparle la cuenta.
- Siempre utilice la salida segura en la página oficial de su entidad bancaria.
- Revise periódicamente sus estados de cuenta y banca electrónica para identificar los posibles reportes negativos.
- Tenga siempre a la mano los números telefónicos para poder reportar o consultar sus transacciones y reporte vía telefónica el riesgo en caso de pérdida o robo de documentos de identificación.
- No entregue o registre información personal o datos de sus cuentas bancarias, por medio de encuestas telefónicas, redes sociales, centros comerciales o al ofrecerle supuestos premios o servicios.
- Solicite a través del buró de crédito, su historial crediticio y verifique la existencia de créditos a su nombre y que empresas han consultado su historial crediticio.