BANCO POPULAR

GERENCIA DE RIESGOS NO FINANCIEROS Y CUMPLIMIENTO

CARTILLA DE SEGURIDAD PARA NUESTROS CLIENTES

Recomendaciones para protegerse de ciertos riesgos generados por la utilización de los servicios Bancarios.

Última Actualización: Octubre de 2016
Versión 1.4.

Contenido:

ADVERTENCIA

Las siguientes recomendaciones son tomadas de autoridades a nivel nacional e internacional. Son únicamente una guía educativa para protegerse de ciertos riesgos generados por la utilización de los servicios Bancarios. Por lo tanto, la información aquí presentada no genera ningún tipo de obligación entre el Banco Popular y sus clientes, ni garantiza que su aplicación desaparezca la posibilidad de ocurrencia de fraudes y/o irregularidades. El Banco Popular tampoco se responsabiliza por las decisiones que se adopten con base en esta información.

1. Seguridad en Cajeros Automáticos

Recomendaciones para estar más seguro con sus tarjetas Débito y Crédito del Banco Popular en Cajeros Automáticos.

El Banco Popular cuenta a nivel nacional con más de 1100 cajeros como parte de la Red de 3800 Cajeros Automáticos ATH, los cuales prestan un servicio ágil y sencillo para realizar sus transacciones monetarias.

¿Cómo puede ser victima de los delincuentes en los cajeros?

1.1. Skimming

El Skimmig ó Clonación, consta de la copia de la Banda Magnética y de la clave de la tarjeta. Para este efecto los delincuentes colocan elementos en el lector de las tarjetas de los cajeros, que permiten copiar los datos de la misma. Como ello no es suficiente, colocan cámaras encima del teclado, lo que les permite capturar la clave introducida.

1.2. Cambiazo

En este caso intervienen generalmente dos personas, quienes se ubican en un Cajero Automático para vigilar a los clientes que ingresan allí, en este momento se presentan como personas que quieren ayudar y orientes ó como empleados del Banco y ofrecen ayuda en el manejo del mismo, solicitándoles la tarjeta, la clave y la cantidad de dinero a retirar.

Al momento de devolver la tarjeta se la cambian al cliente con otra similar, de otro cliente que han estafado ó una falsa. Posteriormente, con la clave memorizada ó anotada y la tarjeta, proceden a realizar retiros de la cuenta.

1.3. ¿Cómo protegerse ante estos eventos?

- ✓ Antes de introducir la tarjeta en el cajero, verifique que no existan elementos extraños dentro del lector que pueda afectar su transacción.
- ✓ No permita que su clave sea observada por personas extrañas al momento de digitarla en un cajero automático ó punto de venta.
- ✓ Al momento de digitar su clave, cubra el teclado con su mano ó de cualquier forma que le sea posible.
- ✓ No preste su tarjeta ni su clave.
- ✓ Si observa cualquier situación sospechosa en el cajero no realice la transacción.
- ✓ Cuando reciba la clave de su tarjeta débito ó crédito, memorícela y destruya inmediatamente la Pin Card correspondiente.
- ✓ Nunca guarde la tarjeta junto al documento de identidad, ni la guarde junto con la clave.
- ✓ Nunca suministre su clave ni su número de cuenta a personas que se la soliciten bajo ningún tipo de argumento, en especial la participación en concursos, premios ó cualquier tipo de oferta.
- ✓ Nunca acepte ayuda de terceros.
- ✓ Si debe salir rápidamente de un cajero electrónico, presione la tecla cancelar.
- ✓ Cambie la clave de su tarjeta periódicamente y no la escriba en un lugar cerca de la misma, ni al reverso.
- ✓ Nunca acepte ayuda con teléfonos celulares para que llame a su banco.
- ✓ Tenga presente el número de teléfono para bloquear la tarjeta en caso de pérdida.

2. Seguridad en Establecimientos de Comercio

Recomendaciones para la utilización segura de las tarjetas en establecimientos de comercio.

¿Cómo puede ser victima de los delincuentes en los establecimientos de comercio?

2.1. Cambiazo

En este caso, al momento de devolverle la tarjeta se la cambian con otra similar, de otro cliente al que han estafado ó una falsa. Posteriormente con la clave memorizada ó anotada y la tarjeta, proceden a realizar retiros de la cuenta del cliente.

2.2. ¿Cómo protegerse ante estos eventos?

- ✓ Cuando vaya a realizar una compra en establecimientos comerciales con cualquiera de sus tarjetas, entréguela únicamente al encargado de hacer la transacción en la caja y no lo pierda de vista a él, ni su tarjeta.
- ✓ Nunca permita que deslicen su tarjeta en aparatos diferentes a los definidos para el pago (Datáfonos).
- ✓ No olvide su tarjeta después de realizar el pago.
- ✓ Verifique el monto de la compra.
- ✓ Destruya los comprobantes de pago de sus compras, antes de arrojarlos a la basura.

3. Seguridad en Nuestra Red de Oficinas

Cuando visite nuestras oficinas, hágalo con seguridad.

¿Cómo puede ser víctima de los delincuentes en las oficinas?

3.1. Fleteo

Es una práctica muy común en la cual la persona que acaba de retirar una gran suma de dinero de una oficina bancaria es robada a mano armada por individuos en automóvil ó motocicleta.

3.2. Cambio de Títulos Valores por Efectivo

Es una modalidad destinada a inducir el cambio de cheques por efectivo de aquellas personas que se encuentran en las filas, los cuales posteriormente adulteran su valor y se cometen estafas a terceros.

3.3. Suplantación de empleados del Banco

A través de este mecanismo personas inescrupulosas buscan recibir de los clientes dinero por fuera de la caja de la oficina, haciéndose pasar por funcionarios del Banco.

3.4. ¿Cómo protegerse ante estos eventos?

- ✓ Abstenerse de retirar altas sumas de dinero en efectivo, es recomendable solicitar cheques de Gerencia ó efectuar transferencias electrónicas.

- ✓ Si lo anterior no es posible, cuando se van a efectuar retiros de altas sumas de dinero de una entidad financiera, procure no informar a ningún empleado, familiar ni persona desconocida ó que le genere suspicacia, este debe ser un hecho confidencial. Sin embargo, cuando retire el dinero hágalo acompañado de personas de confianza.

- ✓ Si se presentan demoras injustificadas en la entrega del dinero que hayan obligado al cajero a retirarse del lugar y realizar llamadas telefónicas, se debe informar de inmediato al Gerente de la Oficina del Banco.

- ✓ Mientras espera la entrega del dinero, observe la actitud de las otras personas, especialmente de clientes que se encuentren a su alrededor, ya que muchos delincuentes se ubican dentro de las filas para observar quienes retiran dinero y poderlos atacar en la vía pública.

- ✓ Al realizar trámites con cierta periodicidad, evite crear rutinas que permitan conocer días, y horarios de sus movimientos bancarios.

- ✓ Si detecta personas sospechosas informe a las autoridades o personal de seguridad.

- ✓ Tenga en cuenta que en los Bancos el único sitio para la recepción y entrega de dinero en efectivo, son las cajas, si se acercan personas que dicen ser funcionarios del Banco y ofrecen hacer transacciones de depósito ó pago en efectivo, avise de manera inmediata a uno de los funcionarios ubicados en las áreas de atención de la oficina.

- ✓ No revele a extraños su información.

- ✓ No solicite ni reciba ayuda de extraños, solicítela únicamente a personal de la entidad.

4. Seguridad en Internet

No se descuide, Manténgase alerta con el robo de identidad y el fraude en Internet.

¿Cómo puede ser victima de los delincuentes en Internet?

4.1. Robo de Identidad

El Término Robo de Identidad se refiere a todos los tipos de delitos en los cuales un individuo obtiene y utiliza ilícitamente los datos personales de otra persona, como por ejemplo su nombre, número de cédula, número de tarjeta de crédito u otra información de identificación, de tal forma que implica fraude ó engaño, generalmente para beneficio económico.

¿Cómo se realiza el Robo de Identidad?

- ✓ Robo de la Billetera ó Bolso.
- ✓ **Skimming**, Robo de números de tarjetas débito y/o crédito, capturando la información mediante dispositivos de almacenamiento de datos. (Ej.: copiado de la información de la banda magnética).
- ✓ Revisión de la Basura.
- ✓ Robo de Correspondencia.
- ✓ Robo de información personal en la casa.
- ✓ **Phishing**, correos electrónicos fraudulentos.
- ✓ **Vhishing**, Llamadas fraudulentas.
- ✓ **Pharming**, **Malware**, Software Malicioso, Piratería Informática.

¿Qué pueden hacer con la información robada?

- ✓ Abrir nuevas cuentas bancarias ó solicitar tarjetas de crédito.

- ✓ Solicitar créditos bancarios.
- ✓ Adquirir servicios de telefonía celular.
- ✓ Falsificar tarjetas débito ó crédito.
- ✓ Realizar transferencias electrónicas.
- ✓ Obtener otros documentos de identidad de manera fraudulenta.

Entre otros, y todo lo anterior en nombre de la persona a la cual le fue robada la identidad.

4.2. Ingeniería Social

La ingeniería social es el método más utilizado para realizar el robo de identidad en Internet. La ingeniería social es la práctica de obtener información confidencial a través de la manipulación de usuarios legítimos. Un ingeniero social usará comúnmente el teléfono ó Internet para engañar a la gente y llevarla a revelar información sensible, o bien a violar las políticas de seguridad típicas, antes que aprovechar agujero de seguridad en los sistemas informáticos.

4.3. Estrategias de la Ingeniería Social

4.3.1. Phishing

Se caracteriza por intentar adquirir información confidencial del cliente de forma fraudulenta, para luego realizar estafas y robos con dicha información.

El estafador ó phisher, se hace pasar como persona ó empresa de confianza en una aparente comunicación electrónica oficial, por lo común un correo electrónico ó algún sistema de mensajería instantánea, en el cual se inserta un “link” ó vinculo a una página de Internet que a primera vista parece la verdadera, pero realmente es una imitación de la página real, así el cliente confía en el portal visitado cuando en realidad se encuentra en otro sitio.

4.3.2. Vishing

En este caso el estafador tiene un software que le permite llamar a muchos números telefónicos de una determinada región.

Cuando la llamada es contestada, suena una grabación y alerta a la persona que su cuenta, tarjeta de crédito, etc., está siendo utilizada de forma fraudulenta y que debe llamar al número que sigue inmediatamente. El número puede ser un número gratuito falso de la compañía financiera que se pretende representar.

Una vez la victima llama a este número, el teléfono es contestado por un software que le indica al “cliente” que su cuenta necesita ser verificada y que requiere que ingresen la información confidencial.

4.3.3. Malware ó Programa Malicioso

Son programas ó archivos dañinos para los computadores, estos están diseñados para insertar virus, Spyware, entre otros. Quizá con el propósito de recoger información sobre el usuario o sobre el computador en sí.

4.3.4. Hijacker

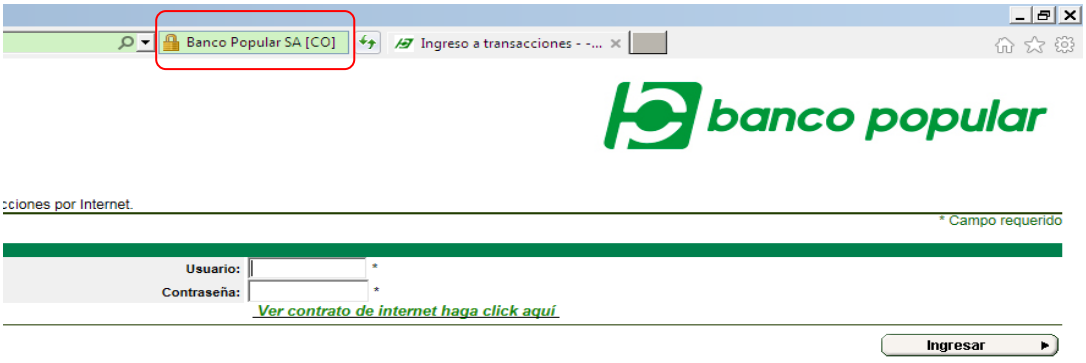
Es un tipo de software que realiza cambios en la configuración del portal de inicio del navegador de Internet, que lo redirige a otras páginas de características indeseables como son las pornográficas y más peligrosamente a copias casi fieles de las bancarias.

4.4. ¿Cómo protegerse ante estos eventos?

- ✓ Nunca responda a solicitudes de información personal a través de correo electrónico. Las empresas nunca solicitan contraseñas, números de tarjeta de crédito u otro tipo de información personal por correo electrónico. Si recibe un mensaje que le solicita este tipo de información, no responda e informe el hecho.

- ✓ Al visitar sitios Web, introduzca la dirección en el sitio en la barra de direcciones del navegador de Internet, nunca de click a un enlace “link” que le envían en un correo para acceder. Estos pueden conducirlo a un sitio falso que enviará toda la información registrada al estafador que lo ha creado.

- ✓ Cerciórese de que el sitio Web es seguro, antes de ingresar cualquier tipo de información personal, compruebe si el sitio Web utiliza cifrado para transmitir la información personal, en Internet Explorer puede verificarlo si aparece un icono de color amarillo en forma de candado situado al lado de la barra de direcciones.



- ✓ Para comunicarse con su entidad financiera, marque los números telefónicos publicados en el directorio telefónico.

- ✓ Nunca entregue información personal a “alguien” que llame a su teléfono. Si cree que es necesario retorne la llamada a los números de confianza.

- ✓ Cuando realice transacciones por Internet, trate de realizarlos desde sitios conocidos, por ejemplo su casa, su oficina ó centros de Internet del banco Popular. Evite realizarlas desde sitios públicos, como Café Internet ó Computadores Compartidos que son usados por varias personas.

- ✓ Tenga un antivirus y un antispyware instalado en su computador, actualícelo constantemente.

- ✓ Nunca suministre información personal (claves secretas, números de cuentas, números de tarjetas de crédito y/o débito, documentos de identidad) a personas que se lo soliciten bajo el argumento de participar en concursos, premios ó cualquier otro tipo de oferta.

- ✓ Cuando termine sus transacciones y operaciones cierre cada sesión, nunca abandone el computador mientras esté en medio de sesión abierta ó una transacción iniciada.

5. Seguridad en Línea Verde y Banca Móvil

Otras recomendaciones a tener en cuenta para proteger su seguridad

El Banco Popular le permite realizar transacciones por otros canales como son la Línea Verde y la Banca Móvil. En ellos existe también el riesgo de que su información pueda ser utilizada por terceros y utilizada para realizar fraudes.

5.1. ¿Cómo protegerse ante estos eventos?

- ✓ No preste su celular a un desconocido, allí usted puede tener información comercial, sobre las alertas que recibe y las transacciones que realiza en su celular.
- ✓ Evite utilizar celulares ajenos para realizar operaciones telefónicas. Solo inscriba celulares sobre los cuales tenga control en la realización de transacciones.
- ✓ En lo posible elimine de su celular los mensajes de alerta, que contengan información personal ó financiera, una vez hayan sido leídos por usted.

- ✓ Si realiza sus operaciones de Línea Verde a través de un teléfono con pantalla digital, verifique que la información que digitó no quede almacenada en el teléfono, lo cual puede verificar pulsando la tecla “Redial”. En caso de que alguna información quede registrada marque otro número, y así la información podrá eliminarse.

- ✓ Evite utilizar servicios telefónicos de cabinas públicas ó minutos de celular de la calle.

- ✓ Evite utilizar el altavoz del teléfono, alguien puede escuchar su información financiera.

6. Bloqueo de Productos y servicios

PRODUCTO	TELEFONO	HORARIO
Tarjeta de Crédito	6063456	Lunes a Domingo, las 24 Horas del día
Tarjeta Débito	6063456	Lunes a Domingo, las 24 Horas del día
Cuentas de Ahorro ó Corrientes	6063456	Lunes a Domingo, las 24 Horas del día

7. ¿Requiere mayor información sobre estos temas?

El Banco Popular ha dispuesto el correo electrónico **segurinfo@bancopopular.com.co** y el **teléfono 3395500 Ext. 4708**, para obtener mayor información acerca de éstos y otros temas de seguridad.

Banco Popular

Gerencia de Riesgos no Financieros y Cumplimiento
Dirección de Seguridad de la Información

Octubre de 2016