INFORMACION UTIL

BANCO PICHINCHA

Recomendaciones de Seguridad

PORTAL INTERNET

Existen varias modalidades de fraude por internet, entre las más frecuentes se encuentran:

- **El phishing** es una técnica de captación ilícita de datos personales y de cuentas bancarias a través de enlaces de correos electrónicos o páginas Web, que suplantan la imagen de una entidad financiera.
- **Pharming** es la explotación de una vulnerabilidad en el software de los servidores DNS (Domain Name System) o en el de los equipos de los propios usuarios, que permite a un atacante redirigir un nombre de dominio (domain name) a otra máquina distinta. De esta forma, un usuario que introduzca un determinado nombre de dominio que haya sido redirigido, accederá en su explorador de internet a la página web que el atacante haya especificado para ese nombre de dominio.

Para prevenirlos:

- Utilice contraseñas fuertes con símbolos, números, mayúsculas y minúsculas, procure cambiarlas periódicamente.
- Memorice las contraseñas, no utilice la opción de almacenar que ofrece el navegador.
- Teclee siempre usted mismo la dirección de la página Web de la Entidad, el único sitio autorizado para ingresar a la Entidad es www.bancopichincha.com.co
- Verifique que la dirección electrónica a la que está accediendo empieza con las siglas "https", es decir, que además cuenta con una letra "s".
- No siga enlaces que se encuentren en correos electrónicos aunque vengan de alguien conocido, mensajería instantánea o banners, que le podrían conducir a páginas falsas de la Entidad Financiera.
- Evite realizar transacciones en lugares de concesión pública a Internet.
- Valide siempre que en la parte superior o inferior del navegador aparezca el icono de un candado cerrado. De lo contrario no realice ninguna transacción.
- Al finalizar una transacción por Internet asegúrese de cerrar la sesión y borrar los archivos temporales.
- Recuerde que el BANCO PICHINCHA, NUNCA lo contactará para solicitarle información confidencial como las contraseñas de sus cuentas, a través del teléfono, del correo electrónico o de cualquier otro medio.
- Actualice las opciones de seguridad de su computador y antivirus utilizando herramientas de seguridad adecuadas (antivirus, antispyware, firewall, etc.).
- Nunca preste su cuenta bancaria para recibir fondos cuyo origen usted desconoce, delincuentes utilizan este método para la transferencia de dinero de procedencia ilícita.

CALL CENTER

Las modalidades de fraude más frecuente tienen como propósito la obtención de la información del cliente para fines fraudulentos.

- **Vishing,** utiliza mensajes de correo fraudulentos que sugieren llamar a un número de teléfono, en el cual un contestador automático va solicitando toda la información requerida para acceder a nuestros productos a través de medios electrónicos.
- **Smishing,** utiliza el envío de mensajes SMS de los teléfonos móviles, los mensajes intentan convencer del ingreso a un sitio web falso o a un sitio de audio respuesta en el cual le solicitarán sus claves.

Para prevenirlos:

- Recuerde que su clave telefónica es personal e intransferible.
- Nunca digite su clave telefónica en presencia de otras personas.

- Cambie su clave periódicamente.
- Al asignar su clave, preferiblemente no utilice su año de nacimiento ni los dígitos de su cédula.
- Verifique que al marcar la tecla redial en teléfonos con pantalla, no quede almacenada la información digitada (Número de identificación, clave, etc.).
- Evite realizar consultas desde cabinas telefónicas públicas.
- Procure no utilizar teléfonos celulares de personas desconocidas.
- No permita la ayuda de terceros para realizar sus consultas o transacciones, éstas las debe realizar el titular de la cuenta o producto.

CAJEROS AUTOMATICOS

Las modalidades más frecuentes de fraude son:

- **Skimming, copiado de banda** por medio de dispositivos falsos instalados en los cajeros.
- **Robo de clave por medio de cámaras** instaladas para visualizar el teclado.
- **Robo de clave por personas desconocidas** que ofrecen ayuda en el uso del cajero o están cerca para observar su clave personal.
- **Cambiazo**, personas que le ofrecen ayuda y le cambian la tarjeta.
- **Trampas**, cuando se instalan elementos extraños que impiden la dispensación del dinero o copiar la banda de la tarjeta.
- Pérdida de confidencialidad de la clave (PIN).

Para prevenirlos:

- No informe su clave a terceros por ningún medio.
- Revise periódicamente si tiene las tarjetas en su poder.
- Sea consciente de los sitios y sus alrededores cuando retire dinero. Si observa algo anormal, vuelva más tarde o utilice otro cajero automático.
- Bloquee con su cuerpo y manos la visión de otros sobre la pantalla y teclado del cajero, así evitará que alguien más conozca su clave.
- Si el cajero no le entrega el dinero y el recibo indica que la operación fue exitosa, repórtelo de inmediato a la oficina respectiva o llamando a nuestro Call Center.
- Si el cajero presenta daños, no acepte ayuda de extraños, en ese caso cancele la operación y reporte el daño a algún funcionario de la Oficina más cercana.
- No utilice cajeros que presenten objetos extraños o alteraciones en su aspecto.
- No introduzca su tarjeta en el cajero si éste se encuentra fuera de servicio.
- Si el cajero retiene su tarjeta, bloquéela inmediatamente llamando a las líneas de Credibanco en Bogotá 3278700-10 o Nacional 018000 918472 o si lo prefiere a nuestro Call Center.
- En caso de ser retenida su tarjeta haga caso omiso de avisos o mensajes para supuesto desbloqueo, donde le soliciten digitar su clave o lo remitan a teléfonos para reportarla.
- Conserve sus comprobantes de pago para que pueda corroborar las operaciones detalladas en el extracto.
- Llévese los recibos para que los posibles criminales no sepan cuánto retiró o cuánto dinero tiene en su cuenta.
- Cuando termine de usar el cajero no se retire hasta que la transacción haya finalizado
- Guarde el dinero y la tarjeta antes de retirarse del cajero automático. Evite mostrar el dinero. Verifique que la cantidad que retiró o depositó corresponda con la cantidad reportada en el recibo.

OFICINAS

Las modalidades de Hurto más frecuentes en las oficinas son:

- **Suplantación de Funcionarios,** medio en el que personas inescrupulosas buscan recibir dinero de los clientes, haciéndose pasar por funcionarios de la Entidad Financiera, irregularidad que se presenta en el Hall Bancario.
- **Atraco en instalaciones o fuera del Banco (Fleteo),** en el que sustraen de manera intimidatoria el dinero que ha sido retirado en efectivo.

Para prevenirlos:

- Evite hablar con extraños en la fila.
- No entregue su dinero o pagos a personas extrañas que se hacen pasar por funcionarios, éstos solo se reciben en caja.
- No solicite ayuda a terceros para el diligenciamiento de los formatos de consignación o retiro.
- Pase a la ventanilla de caja únicamente cuando este desocupada y no permita que otras personas se acerquen a usted cuando esté realizando una transacción.
- Cuando realice retiros en efectivo, cuente el dinero en presencia del cajero y no se retire hasta que lo haya guardado.
- Cuando realice consignaciones en efectivo, no se retire de la ventanilla hasta que el cajero haya registrado completamente la transacción.
- En lo posible no retire grandes cantidades de dinero en efectivo, utilice las opciones de transferencia de fondos.
- Cuando retire dinero por sumas elevadas solicite acompañamiento de la policía llamando al 123 o al CAI más cercano.
- Por seguridad está prohibido el uso de celulares dentro de las instalaciones de la oficina.

CHEQUERAS

Las modalidades de fraude más frecuentes con cheques o chequeras son:

- Hurto de Cheques o Chequeras.
- Falsificación de Cheques y firmas autorizadas.

Para prevenirlos:

- Evite que otras personas tengan acceso a sus cheques y a la información de sus cuentas.
- Cuando reciba su chequera cuente el número de cheques y asegúrese que la numeración sea consecutiva. En caso de tener algún faltante o irregularidad no reciba la chequera y notifíquelo inmediatamente.
- Si autoriza a otra persona a recibir sus chequeras indíquele que lleve a cabo este mismo procedimiento.
- Realice permanentemente inventario de su chequera y valide que no tengan saltos en la numeración.
- En caso de pérdida de la chequera o de uno o varios cheques comuníquese con el Call Center o acérquese a la oficina más cercana para dar orden de no pago y posteriormente poner el respectivo denuncio.
- Verifique que los cheques que reciba no tengan tachaduras o alteraciones en ninguno de sus datos.
- Nunca guarde cheques previamente diligenciados o firmados en blanco.
- Identifique plenamente a las personas a quienes les entrega cheques y de quienes los recibe.

TARJETAS CREDITO, DEBITO Y PREPAGO CASH

- Su tarjeta y clave son personales e intransferibles.
- Memorice su clave, no la escriba ni la cargue en el mismo lugar con sus tarjetas.

- Cambie periódicamente su clave.
- Asegúrese de ingresar su clave correctamente para evitar bloqueos por pin inválido y costos adicionales.
- No preste sus tarjetas para que otras personas efectúen transacciones por usted.
- Verifique sus tarjetas periódicamente para asegurarse que no le falta ninguna.
- No le proporcione su número de tarjeta a terceros por teléfono o a través de Internet.

Precauciones al utilizar sus tarjetas en establecimientos comerciales y Cajeros Automáticos

- Al realizar transacciones no pierda de vista en ningún momento su tarjeta.
- Si el datáfono se encuentra en un punto distante, acompañe al funcionario del establecimiento hasta donde esté ubicado el punto de pago.
- Verifique que el datáfono o el cajero automático se encuentre en perfecto estado, tenga precaución con datáfonos abiertos y/o en mal estado.
- Verifique que no existan materiales extraños en las ranuras del cajero automático.
- No permita que su tarjeta sea leída en ningún otro dispositivo diferente al datáfono.
- Verifique que su tarjeta le haya sido devuelta y valide que no haya sido reemplazada por otra.
- En el momento de digitar su clave en el datáfono o cajero automático, oculte el teclado, para que impida que extraños observen.
- Exija voucher y factura, verifique que el valor de la compra sea igual al monto de la transacción reportada.
- Observe mientras los cajeros procesan su tarjeta y asegúrese que no la pasen electrónicamente por dispositivos distintos, si eso ocurre, póngase en contacto con el Banco.
- Sus tarjetas pueden ser bloqueadas en caso de robo, extravío, digitación de clave errada en tres oportunidades o por razones preventivas en caso de fraude o uso indebido.

Acciones ante un evento de Seguridad

Si tiene cualquier duda o sospecha informe a nuestro
Call Center Nacional **018000 919918** o en Bogotá al **6501000**,
o escríbanos por correo electrónico a la dirección
clientes@bancopichincha.com.co para tomar las medidas del caso.

Recomendaciones para activar, inactivar, bloquear, desbloquear o cancelar los productos del Banco Pichincha

BLOQUEOS Y DESBLOQUEOS DE CUENTA CORRIENTE Y DE AHORROS

La solicitud de bloqueo o desbloqueo puede hacerse en cualquiera de las oficinas del Banco.

Bloqueo o desbloqueo por solicitud del titular:
- Se lleva a cabo cuando el titular de la cuenta solicita el bloqueo por alguna situación particular.
- Solo quedarán bloqueadas las transacciones débito.
- El bloqueo es de carácter temporal.
- Para desbloqueo debe acercarse a la oficina.
- Debe diligenciar el formato único de novedades no monetarias con firma y huella y presentar el documento de identidad original. Para el caso de Persona Jurídica se podrá recibir carta de solicitud firmada por el Representante legal.

Bloqueo por fallecimiento del titular:
- Se lleva a cabo cuando se recibe la notificación del fallecimiento de un titular de cuenta.
- La cuenta permanecerá en este estado hasta que se realice la entrega a los herederos, previa presentación de los documentos correspondientes y autorización de la Entidad.

INACTIVACION Y REACTIVACION DE CUENTA CORRIENTE Y DE AHORROS

Inactivación de cuentas: La cuenta se inactiva automáticamente cuando no se realizan transacciones débito o crédito durante un tiempo prolongado. El periodo establecido por la Superintendencia Financiera de Colombia es de 180 días.

Este tipo de cuenta no permite transacciones débito por parte del Cliente, pero si permite transacciones crédito.

Sin embargo, es susceptible de transacciones débito automáticas generadas por el Sistema, tales como comisiones, IVA y deducción de impuestos.

Reactivación de cuentas: La activación de una cuenta inactiva o bloqueada puede ser solicitada personalmente por el titular en cualquier oficina de la red del Banco.

CANCELACION DE CUENTA CORRIENTE Y DE AHORROS

El cierre de cualquier tipo de cuenta sólo puede realizarse en la oficina sede de la misma y por el titular del producto. En caso de ser persona jurídica, podrá hacerse con la persona autorizada para tal fin.

El titular debe entregar carta con firma y huella donde solicita el cierre de la cuenta.

Para el caso de cuentas corrientes es estrictamente necesaria la presentación de la chequera para proceder a destruirla o, en su defecto, el denuncio ante la autoridad competente indicando la pérdida de la misma.

BLOQUEO TARJETAS DE CREDITO, DEBITO Y PREPAGO CASH

- El bloqueo de sus tarjetas puede realizarse en caso de robo, fraude, extravío o retención en un cajero automático a través de los siguientes canales:
  - **Red nacional de oficinas:** A través del diligenciamiento del formato respectivo con firma y huella para tarjeta débito y prepago.
  - **Portal de Internet:** Previa validación de la clave.
  - **Call Center:** Línea 018000919918 ó 6501000, previa verificación de los datos básicos.
  - **Credibanco:** Líneas 3278710, 3278600 ó 5466900 en Bogotá.
- El titular de la cuenta, podrá realizar la cancelación o el bloqueo de cualquier tarjeta asociada a la cuenta.
- Los bloqueos de los plásticos son irreversibles e implican la reexpedición de una nueva tarjeta.
- La tarjeta débito y prepago es bloqueada como consecuencia del ingreso errado de la clave, el sistema en forma automática la habilitará 24 horas después del bloqueo.
- El bloqueo de la tarjeta será definitivo por hurto, extravío o fraude, cancelada por el tarjeta habiente o por el banco.
- El titular de una tarjeta de crédito podrá realizar la cancelación o el bloqueo de sus tarjetas principales o amparadas.

CANCELACION TARJETA DE CREDITO

Se podrá cancelar la tarjeta de crédito en cualquiera de las oficinas de la red, pagando la totalidad del saldo y entregando el plástico perforado en la banda magnética o firmando el formato de responsabilidad en caso de no devolverla.

Call Center Bogotá: 650 1000
Nacional: 01 8000 919918 / 01 8000 111111
www.bancopichincha.com.co