BANCO PICHINCHA

Recomendaciones de **Seguridad**

Entérese de como protegerse de los **ataques informáticos.**

Para nosotros la seguridad de la **información de los clientes** es de vital importancia.

Por tal razón lo invitamos a leer este documento, y seguir algunas recomendaciones para evitar ser **víctima de estos fraudes.**

¿Sabe qué son los Cibercriminales?

Son personas que se dedican a cometer todo tipo delitos ya sean:

- **Cibernéticos**
- **Electrónicos**
- **Informáticos**

Con el objetivo de causar daños a los sistemas en busca de algún beneficio.

Modalidad de fraude

1 Ingeniería Social

Es una técnica que utilizan los **delincuentes y cibercriminales** para engañar y manipular a sus víctimas buscando persuadirlas para que realicen alguna acción y capturar información confidencial como **números de cuenta, usuarios, contraseñas, datos personales, datos financieros** y de esta manera cometer otros fraudes utilizando su información, a continuación, mencionamos **algunas de las técnicas de ingeniería social en la que cualquier persona podría ser víctima**:

Cambiazo: Es una modalidad de fraude **dirigida a tarjetas débito o crédito** en la cual los delincuentes distraen a la víctima de diferentes formas con el fin de cambiar la tarjeta real por otra similar.

Clonación: Este tipo de modalidad busca **copiar la información de las tarjetas débito y crédito** por medio de dispositivos que se instalan en los **datáfonos y cajeros automáticos,** para la posterior clonación de las tarjetas y hacer uso de ellas.

Fleteo: Esta modalidad tiene como lugar de operación las oficinas bancarias, el **delincuente identifica la víctima cuando retira sumas grandes de dinero**, con el fin de abordarla y robarla.

Paquete chileno: Esta modalidad de fraude tiene como fuente el **engaño** y su principal lugar de operación son las **oficinas bancarias,** el delincuente simula dejar caer un paquete supuestamente **"con dinero"**, luego se acerca el cómplice a recoger dicho paquete y le pregunta a la víctima si le pertenece, posterior a esto, el cómplice lo convence para que se desplacen a otro lugar fuera de la oficina y hacer la **repartición del supuesto dinero**, cuando se desplazan al lugar acordado el cómplice convence a la víctima para que le entregue **su dinero a cambio del paquete**.

Phishing: Técnica de **ingeniería social que inicia a través de un correo electrónico falso** aparentando ser legítimo, el cual contiene un enlace solicitando ingresar una información confidencial como, **usuarios, claves, datos personales, datos financieros, entre otros**, haciendo pensar a la víctima que está ingresando a una página real y que está entregando sus datos a una entidad confiable pero realmente la está entregando al delincuente.

Vishing: Modalidad usada por los delincuentes en la que **suplantan por medio telefónico** a funcionarios de una entidad confiable del sector **salud, financiero, educativo, gobierno, entre otros**, con el fin de robar información confidencial, como claves, cuentas, datos personales, entre otros.

Smishing: Modalidad usada por los delincuentes en la que **suplantan** entidades confiables del sector **salud, financiero, educativo, gobierno, entre otros,** por medio de **mensajes de texto en el celular (SMS),** con el fin de tomar información confidencial, como claves, cuentas, datos personales, entre otros, generalmente le piden a la víctima que se comunique a un número telefónico o que ingrese a un enlace.

Pharming: Esta modalidad es usada por los **cibercriminales** para instalar **malware en su computadora o dispositivo móvil** con el fin de cambiar las direcciones web de sus sitios favoritos de navegación y engañarlo, haciéndole pensar que ingresa a una página web legítima pero realmente es una página **falsa creada por el ciberdelincuente**.

Malware: Es un **código malicioso**, que se instala en computadoras o dispositivos móviles, el cual puede llegar a realizar diferentes daños, a **continuación, se mencionan los malware más usados por los ciberdelincuentes:**

- **Keylogger:** Después de instalarse en su equipo, capta absolutamente todas las pulsaciones de teclado como usuarios, claves, datos personales, financieros, etc. Generalmente el computador de la víctima se infecta al conectar una USB desconocida en su equipo o en el caso de los dispositivos móviles en la instalación de aplicaciones móviles destinadas para esta finalidad.

- **Rasomware:** También conocido como secuestro de información, se instala por medio de la descarga de un archivo adjunto al correo electrónico que contiene el malware, al ser instalado, cifra toda la información del disco duro imposibilitando la lectura de la misma a la víctima, luego le solicita una suma de dinero (generalmente solicitada en criptomonedas) a cambio de liberar la información nuevamente en su dispositivo.

- **CriptoJacking**: Es usado por los cibercriminales con el fin de tomar control de un dispositivo con el fin de minar (creación de Criptomonedas).

- **Troyanos:** Se instalan en los computadores y realizan diferentes daños a la información almacenada, e inclusive pueden tomar el control total del computador.

Whaling: Esta modalidad de fraude es la **combinación de varias modalidades de ingeniería social** hacia la víctima de manera repetitiva, como el envío de **correos electrónicos, llamadas, mensajes de texto falsos, con el fin de robarle su información.**

Tips de seguridad para nuestros usuarios

Para nosotros es muy importante proteger la información de nuestros **clientes** y la seguridad en las transacciones realizadas a través de los canales de atención que tenemos **dispuestos a su servicio.**

Tenga en cuenta las **siguientes recomendaciones** de seguridad, para que sus transacciones estén siempre protegidas:

1 Seguridad en cajeros automáticos y datáfonos:

- Personalice su **tarjeta en el espacio en blanco** que se encuentra al respaldo, con su nombre o con una marca que la identifique fácilmente.
- NO pierda de vista su tarjeta **cuando realice compras**.
- NO olvide verificar la **presencia de personas sospechosas** a su alrededor.
- Al digitar su clave, **cubra el teclado con la mano** para evitar que cámaras ocultas u otras personas puedan visualizar lo que digita.
- NO reciba ayuda de **extraños** en los cajeros automáticos.
- Revise que no se encuentre **ningún dispositivo extraño en la ranura donde inserta su tarjeta** o un teclado sobrepuesto antes de retirar su dinero en cajeros automáticos.
- Evite retiros de dinero en **sitios riesgosos o en una hora poco apropiada**.
- Si por alguna razón **su tarjeta es retenida en el cajero,** no se retire hasta finalizar o anular la transacción.
- Memorice la clave, no la porte ni la escriba en ninguna parte y **recuerde cambiarla periódicamente**.
- En caso de cancelar la tarjeta **destrúyala raspando la firma**, cortando el plástico en fragmentos y verificando que el **chip quede inservible**.

2 Seguridad de transacciones en internet:

- Evite abrir archivos adjuntos que envían en cadenas, **pueden ser virus**.
- Mantenga **instalado y actualizado** un antivirus.
- Utilice un **computador confiable** para realizar transacciones.
- No se **conecte a redes de acceso público, ni realice transacciones desde computadores públicos,** pues en ellos pueden grabar sus números de cuentas y claves, para sí acceder en su nombre y hacer el fraude.
- Ingrese siempre la dirección de la página web del banco **www.bancopichincha.com.co,** nunca lo haga desde un enlace (link) que le llegue de algún correo electrónico.
- Antes de realizar cualquier transacción verifique que se encuentre el **símbolo del candado,** el cual indica que es una conexión segura.
- Otra característica que indica que se encuentra conectando a un sitio seguro, es que la página de internet inicia **con las letras "https".**

- Al realizar compras online **no ingrese números de tarjetas de crédito o cualquier dato confidencial** antes de validar que está en un sitio seguro.
- Al finalizar sus operaciones en la banca virtual, **no olvide cerrar su sesión**.
- No utilice la opción de los navegadores para guardar sus credenciales de manera automática, **memorícela y digítela en cada ingreso**.
- Mantenga su dispositivo de seguridad **(token)** en un lugar **privado y seguro**, no lo comparta con terceros, **ni permita que este en un lugar visible**.

"Maneje de manera responsable *su información en la web"*

3 Seguridad en su Móvil:

- En lo posible cuente con un **antivirus en su móvil**.
- No se conecte a **redes de acceso público**, como wifi.
- Solo active las conexiones por **Bluetooth y Wifi** cuando vaya a utilizarlas.
- Mantenga su móvil configurado con una **huella**, **contraseña, pin o patrón** para su acceso.
- No acceda a **enlaces recibidos por mensajes de texto de dudosa procedencia**.
- No conecte su **dispositivo móvil a equipos desconocidos** o que no se encuentren protegidos.
- No almacene en notas dentro de su dispositivo móvil, información confidencial como **usuarios, claves, datos personales, financieros, etc**.
- En caso de perder su teléfono celular, **cambie de inmediato las contraseñas e informe al banco**.
- No utilice **teléfonos celulares de terceros para realizar transacciones.**
- No acceda a **enlaces informados a través de mensajes de texto no solicitados** y que impliquen la descarga de contenidos en el equipo.

*"Recuerde que en el celular **lleva toda su información personal,** utilícela de forma adecuada"*

4 Seguridad en oficinas bancarias:

- Haga sus transacciones y entrega de dinero únicamente con el **personal autorizado en las cajas de las oficinas**.
- Evite retirar sumas grandes de dinero, utilice **cheques de gerencia o transferencias electrónicas**.
- Si decide hacerlo, realice el conteo del efectivo directamente en la caja y **solicite el acompañamiento de la policía**.
- Esté **atento a personas con actitud sospechosa** al interior o fuera del banco.
- En caso de observar algo sospechoso o extraño, **dé aviso a los funcionarios del banco**.

5 Seguridad con las claves:

Recuerde que **sus claves son secretas** y que al definirlas deben tener **ciertas características**:

- Utilice **mayúsculas, minúsculas, números y caracteres especiales**.
- No utilice **nombres, fechas de cumpleaños, hobbies o cualquier dato** que sea fácil de adivinar.
- Cámbielas **periódicamente** y **memorícelas**.
- No use al menos las últimas **2 contraseñas que haya utilizado con antelación**.
- No comparta **su clave o contraseñas** con terceros.
- En ningún caso **debe facilitar sus claves a nadie**, incluso, cuando manifiesten solicitarlas en nombre del banco.
- Tenga cuidado con **delincuentes que se hacen pasar por funcionarios de las entidades financieras** para ofrecer premios, promociones o rifas, y como parte del proceso de adjudicación de los mismos, solicitan a los clientes las claves secretas.

Ante cualquier caso de seguridad o dudas comuníquese con la línea de atención **650 1000** en Bogotá o al **01 8000 919918** desde cualquier lugar del país.

6 Banca Móvil:

- No defina claves de **fácil deducción** para acceder al **servicio de Banca Móvil**.
- Nunca pediremos **sus claves de acceso** a los **canales electrónicos** a través de **correos electrónicos o mensajes de texto**.
- Descargue sus aplicaciones únicamente desde las tiendas autorizadas **Google Play** (Android), **App Store** (iPhone – iPad) y **BlackBerry** App World.
- No realice **modificaciones de seguridad** en su dispositivo móvil (**Root, Rooting o Rootear**).
- Defina previamente los **topes transaccionales** acorde con sus necesidades.
- Recuerde finalizar **su sesión correctamente**.

"Tenga en cuenta iniciar ***sesión en dispositivos de su confianza****"*

Síganos en redes sociales como
BancoPichinchaCol