Señor cliente,

Ponemos a su disposición información sobre recomendaciones y sugerencias para un mejor y más seguro uso de su Tarjeta de Débito, y de la operatoria de HomeBanking y en los ATM (Cajeros Automáticos).

INGENIERIA SOCIAL

En el campo de la Seguridad Informática, es la práctica de obtener, a través de la manipulación de usuarios legítimos, acceso a información confidencial o privilegios en los sistemas para realizar algún acto que perjudique o exponga una persona a riesgo o abusos.

Algunas técnicas de Ingeniería Social son:

1. **Phishing**

   Es una forma de engaño mediante el envío de un mensaje fraudulento (anzuelo), proveniente aparentemente de una fuente confiable (p.ej. un sitio WEB o una institución financiera), intentando convencerlo para que revele datos confidenciales (claves, cuentas bancarias, números de tarjeta de crédito, identidades, etc.).

2. **Vishing**

   Consiste en hacer llamadas telefónicas para engañar a las personas y obtener información personal o financiera.

3. **Skimming**

   Se denomina así al robo de información de tarjetas de crédito o débito (copiado de la banda magnética) hecho en el momento de la transacción, con la finalidad de reproducir o clonar la tarjeta para su posterior uso fraudulento.

   Los lugares usuales en los que se puede realizar skimming son restaurantes, bares, estaciones de servicio o en cajeros automáticos.

   En el caso de un cajero automático, el autor del fraude pone un dispositivo en el ATM en combinación con una microcámara que graba el PIN (clave) del usuario.

   Normalmente estas acciones se detectan cuando el fraude está consumado.

4. **Robo de Identidad**

   Consiste en obtener y usar datos confidenciales de una persona con un fin ilícito, generalmente para cometer fraudes económicos. Implica la adopción de la identidad de alguien, mediante la información que el delincuente obtuvo de su víctima.

   La mayoría de las veces este delito se advierte una vez consumado, al llegar los débitos de compras que no se hicieron en los resúmenes de cuenta, o se recibe información sobre préstamos, créditos o productos que nunca se solicitaron.

CÓMO PREVENIR RIESGOS EN ACCIONES DE INGENIERIA SOCIAL

Sin ser taxativo, se mencionan una serie de recomendaciones para evitar o disminuir los riesgos mencionados vinculados a Ingeniería Social:

- Si recibe un correo electrónico que le pide información personal o financiera, no lo responda.
- Si tiene alguna duda contacte a la institución que supuestamente le envió el mensaje.
- Si el mensaje que solicita información personal o financiera lo invita a acceder a un sitio web a través de un enlace incluido en su contenido, no lo haga.
- No envíe información personal usando mensajes de correo electrónico.
- Proteja su información personal de miradas indiscretas, sobre todo cuando esté en lugares públicos.
- Tenga cuidado al escribir usuarios y/o contraseñas cuando alguien esté observando, y si hay que hacerlo, que sea rápido
- Controle regularmente sus resúmenes de cuenta, para detectar cualquier transacción irregular o que usted no haya hecho. De detectar algo sospechoso denúncielo de inmediato.
- Nunca envíe por correo electrónico o por teléfono celular números de tarjetas de crédito o cualquier otra información personal o financiera.
- Nunca conteste automáticamente mensajes de correo que soliciten información personal o financiera
- Nunca brinde información personal o financiera por teléfono

CONTRASEÑAS SEGURAS

La Tarjeta de Débito tiene una contraseña (PIN) de cuatro dígitos, totalmente secreta, que es la clave que asegura que ninguna otra persona pueda utilizarla.

Una buena contraseña es vital para la seguridad y para la confidencialidad de la información, por lo que le sugerimos:

- Cree contraseñas robustas, y no las comparta. No guarde las claves, intente memorizarlas
- Si el sobre en el que se recibe el PIN del Banco se encuentra con signos de haber sido violentado, no utilice la tarjeta y realice la denuncia de inmediato en el Banco
- No use contraseñas que sean palabras del diccionario, aunque sea en otro idioma, ni nombres como el del usuario, familiares, mascotas, etc.
- Nunca comparta la contraseña, y si lo hace cámbiela inmediatamente. Tampoco pida la contraseña a nadie.

- No use contraseñas totalmente numéricas con algún significado como números telefónicos, DNI, fecha de nacimiento o una escala numérica ascendente (ej. 123456), etc.

- Cree contraseñas únicas y evite usar el mismo PIN para diferentes aplicaciones.
- De ser factible defina contraseñas que mezclen caracteres alfanuméricos con mayúsculas, minúsculas y símbolos (%&?$).
- Procure que, como mínimo, la contraseña contenga ocho (8) caracteres.
- Deben ser fáciles de recordar para evitar verse obligado a escribirlas.
- No anote la contraseña en ningún sitio ni la escriba si alguien está observando
- No escribir ni pegar el PIN en la misma tarjeta.
- No la envíe por correo electrónico ni la mencione en una conversación
- No mantenga una contraseña indefinidamente, es recomendable cambiarla en forma periódica, independientemente de los cambios que determinados sistemas le exigen con determinada frecuencia.
- Nadie necesita su PIN. Nunca comente su clave, aún si fuera requerido por un funcionario del Banco. Ninguna persona está habilitada para requerir su clave.
- Cuando ingrese el PIN en un cajero automático, tome la precaución que no haya alguna persona tratando de visualizarlo.
- No habilite la opción de “recordar contraseña” en los programas que utilice

HOMEBANKING

Le sugerimos las siguientes recomendaciones para un uso más eficiente y seguro de la plataforma de HOMEBANKING:

- Acceda al HOMEBANKING directamente en la barra del explorador. Nunca siga links.
- El Banco le entrega una tarjeta de coordenadas (grilla de números) para usar con transacciones que requieran doble factor de autenticación.
- Evite ingresar a HOMEBANKIG desde redes públicas como cybers o restaurantes.
- Recuerde siempre utilizar la función “salir” cuando haya terminado de operar. Cierre la sesión del HOMEBANKING y del navegador.
- Recuerde que nunca el Banco solicita datos personales (número de cuenta, nombre de usuario, clave de acceso) vía correo electrónico o llamadas telefónicas.
- Evite miradas indiscretas de terceros que puedan ver la operatoria realizada en HOMEBANKING.
- Mantenga actualizado el software de la PC o notebook
- Instale en su PC o notebook programas de seguridad (firewalls, antivirus y anti spyware) y manténgalos actualizados

- Recuerde que el Banco no envía correos electrónicos (e-mail), ni realiza llamadas telefónicas para solicitar cambio o confirmación de datos personales (número de cuenta, nombre de usuario, clave de acceso, etc.).

PRECAUCIONES RELACIONADAS CON LA TARJETA DE DÉBITO

- La tarjeta de débito es el elemento que identifica al usuario dentro del sistema.
- Guarde su tarjeta en un lugar seguro y verifique la existencia de la misma periódicamente.
- No preste la tarjeta a otra persona.
- Recuerde retirar la tarjeta al finalizar la operación en el cajero.
- Si la tarjeta es retenida por un cajero automático sin un motivo aparente, comuníquese de inmediato con el Banco.
- En caso de pérdida o robo, denúncielo en forma inmediata al Banco.
- Cuando use su Tarjeta de Débito en un comercio, trate de no perder de vista el plástico, para evitar su posible cambio, y que luego se puedan realizar operaciones fraudulentas con su tarjeta.

PRECAUCIONES RELACIONADAS CON EL ASPECTO DEL CAJERO AUTOMÁTICO (ATM)

- Si la boquilla donde se introduce la tarjeta presenta elementos extraños (plástico, hilo u otros), no opere allí, diríjase a otro cajero y comuníquese con la Entidad Financiera.
- Si el teclado donde se ingresan los datos presenta un aspecto anormal (en su composición o tamaño) dirigirse a otro cajero y comunicarse con la Entidad Financiera.
- Al usar cajeros automáticos que se encuentren aislados, especialmente de noche, mire alrededor. Si el cajero automático se encuentra mal iluminado o está en un área escondida, busque otro.

PRECAUCIONES RELACIONADAS CON LA OPERATORIA EN UN CAJERO AUTOMATICO (ATM)

- No ingresar la tarjeta si el ATM se encuentra fuera de servicio.
- Tenga lista la tarjeta y asegúrese que nadie pueda ver cuando se ingresa el número de identificación personal (PIN) o el importe de la transacción.
- No contar el dinero mientras se está en el cajero automático: guardar el dinero, la tarjeta y el recibo de inmediato.
- Siempre tomar el recibo y llevarlo. Conservar los recibos de los cajeros automáticos para compararlos con el estado de cuenta mensual. Es la mejor manera de cuidarse de fraudes.

- No dialogar ni aceptar sugerencias de personas extrañas en el lobby del ATM para realizar operaciones.
- Ante la pérdida de la tarjeta, contactar de inmediato a la Entidad Financiera que emitió la misma.