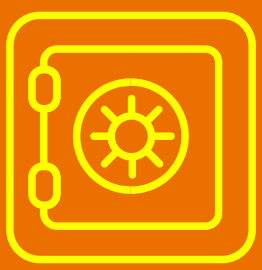
Itaú

Itaú explica todo

Para que te quedes

SIEMPRE
Seguro

NUNCA
víctima de fraude



Cuando el fin es tu seguridad, no existe término medio.

La protección de tus datos bancarios y personales es muy importante para nosotros. Por eso, hemos preparado este libro electrónico que contiene consejos de seguridad e información detallada sobre las estafas más practicadas en la actualidad.

Para que entiendas mejor en qué ambientes y circunstancias ocurren, encontrarás el contenido separado por pilares.

Fraude con tarjetas:

Fraude con falsos funcionarios:

Fraude por WhatsApp:

Fraude de phishing:

(busca robar tu información)

Tips de Seguridad de la Información y Ciberseguridad

Fraude con Tarjetas

Fraude Entrega De Tarjeta

Consiste en que falsos vendedores se quedan con tu tarjeta y te la cambian por otra.

Evita
que alguien más vea la clave que estás digitando al ingresar tu tarjeta.

Procura
Procura no perder de vista tu tarjeta.

Revisa los datos
de la tarjeta devuelta para asegurarte de que sea la tuya.

Te contamos sobre el fraude a tarjetas

¿Cómo pasa?

El estafador aprovecha tu distracción durante el pago en el datáfono, toma tu tarjeta para pasar la compra y te devuelve otra después del pago, conservando tu tarjeta física y todos los datos de la tarjeta.

¿Cómo puedes evitarlo?

Cuando compres en establecimientos, especialmente en tiendas, restaurantes, supermercados, bares, clubes y grandes eventos, verifica siempre el nombre en la tarjeta que se te devolvió para asegurarte de que no te la hayan cambiado.

Fraude intercambio de tarjeta en el cajero automático

Evita recibir ayuda de un desconocido. Si necesitas apoyo para realizar alguna transacción en el cajero, acude a un funcionario de la sucursal bancaria.

Procura estar siempre atento por si alguien está observando tus movimientos.

¿De qué se trata?

En los cajeros automáticos, los delincuentes se aprovechan de tu falta de atención para robar tu tarjeta.

¿Cómo pasa?

Al notar que tienes dudas sobre el funcionamiento del cajero automático, el delincuente te ofrece ayuda y en ese momento, sin que te des cuenta, hace el cambio, te quita tu tarjeta y te entrega otra muy similar a la tuya.

¿Cómo puedes evitarlo?

Cuando tenga dudas sobre el funcionamiento de un cajero automático, no pidas ni aceptes ayuda de nadie en el espacio del cajero automático. Busca siempre a un funcionario dentro de la sucursal bancaria.

Fraude compras no presenciales con tarjeta

Evita que algún tercero vea el número, fecha de vencimiento, nombre y código de seguridad de tu tarjeta.

Mantén siempre tu tarjeta y datos personales en un lugar seguro.

¿De qué se trata?

Esta estafa ocurre cuando los delincuentes usan los datos impresos en tu tarjeta física para realizar compras en tiendas en línea.

¿Cómo pasa?

Con lo que está registrado en la tarjeta: Nombre, número de tarjeta, fecha de vencimiento y código de seguridad, realizan compras en línea, cuando no es necesario tener la tarjeta física para realizar transacciones.

¿Cómo puedes evitarlo?

Nunca des los datos de tu tarjeta a nadie, ya sea por correo electrónico, teléfono, WhatsApp, redes sociales o SMS. No entregues tu tarjeta a otra persona. Recuerda que la tarjeta es de uso personal. Utiliza el pago por enfoque Contact Less. Verifica constantemente la recepción de las alertas de Seguridad o alertas transaccionales, las cuales son notificadas vía SMS o a correo electrónico.

Fraude extravío de tarjeta

Evita desbloquear la tarjeta antes de que llegue.

Permanece atento a la fecha límite informada, si no recibes la tarjeta comunícate inmediatamente con el banco.

¿De qué se trata?

Esta estafa ocurre cuando los delincuentes roban la tarjeta en el proceso de entrega entre el banco y tu dirección.

¿Cómo pasa?

En el camino entre el banco y la dirección de entrega, la tarjeta es interceptada por estafadores que, con sus datos en mano, acceden a los sitios de registro y consultan información como teléfono, fecha y ciudad de nacimiento y nombres de los padres. A partir de ahí, se ponen en contacto contigo haciéndose pasar por el banco y te informan que hubo un problema con la entrega o que, para continuar con el proceso, debes desbloquearlo a través de la aplicación o línea bancaria. Después de que se realiza el desbloqueo, los estafadores usan la tarjeta para realizar compras en tu nombre.

¿Cómo puedes evitarlo?

Nunca desbloquees una tarjeta sin recibirla físicamente. Si solicitas una tarjeta y no la recibes dentro del plazo indicado, infórmalo al banco de inmediato. Nunca te pediremos que desbloquees una tarjeta que no hayas recibido.

Fraude falso motorizado

El banco nunca va a buscar tu tarjeta o el chip.

Mantente atento al recibir llamadas indicando que es del Banco Itaú y solicitando el número de la tarjeta y la clave.

¿De qué se trata?

Un estafador roba tu tarjeta y luego la utiliza en acciones fraudulentas en tu nombre.

¿Cómo pasa?

El fraude ocurre en cuatro etapas:

1. Recibes una llamada en el teléfono fijo, de parte de Itaú o de control transaccional, informándote que se han producido transacciones sospechosas con tu tarjeta.

2. En esta llamada, en un momento determinado, te guían a llamar en el teléfono impreso en el reverso de la tarjeta.

3. Ahí es cuando ocurre la estafa: sin que te des cuenta, el estafador finge colgar, pero permanece en la línea, por lo que se obstruye la llamada y puede oírte llamar al Contact Center. Cuando respondes, crees que estás hablando con nuestro Contact Center, ya que se simulan varios aspectos del Contact Center real, como la música, los mensajes e incluso el propio menú de servicio.

4. Luego, se te pide que cortes tu tarjeta por la mitad y se la entregues a la persona que lo recogerá, ya que dicen que el banco la necesita para realizar el proceso de bloqueo.

¡Importante!

En algunos casos, los estafadores también te piden que les des el chip de tu teléfono celular o incluso tu computadora o tableta. Nunca se los des a nadie.

Fraude falso funcionario

Fraude falso funcionario

Evita dar tu contraseña e información personal en llamadas o mensajes que recibas.

Permanece siempre atento a las llamadas o mensajes que recibes en nombre de Banco Itaú.

¿De qué se trata?

Esta estafa tiene como objetivo hacer que hagas cualquier tipo de movimiento en tu cuenta para enviar dinero a estafadores sin que te des cuenta

¿Cómo pasa?

Una persona te llama y se identifica como gerente o funcionario en un área específica de Itaú. Esto puede suceder mediante una llamada o un mensaje a través de WhatsApp. Actuará para hacer que muevas tu cuenta.

¡Importante!

Para que muevas tu cuenta, los estafadores generalmente informan lo siguiente:

- Hubo un crédito inadecuado en su cuenta. En este caso, el estafador te pedirá que realices el contracargo, es decir, que devuelvas el monto recibido en tu cuenta y, para ello, te pedirá que realices una transferencia al titular y cuenta que se informará en el momento de la llamada.

- Hay un problema con su cuenta o Token. Te aconsejarán que realices transacciones, como transferencias a otras cuentas, como una forma de

"probar" tu cuenta, alegando que los montos volverán a su cuenta al final del día o dentro de las 24 horas, lo que en realidad no sucederá.

- Migración de segmento de cuenta. El estafador te dirá que estás siendo invitado por el banco para ser cliente de otro segmento y que, para que esto suceda, debes transferir el monto que tienes en la cuenta de ahorros a una cuenta informada por él durante la llamada.

¿Cómo puedes evitarlo?

Nunca realices movimientos en tu cuenta, tales como: transferencias, Pagos PSE, pago de fianzas o registro de beneficiarios, a solicitud de cualquier persona, en nombre de Itaú. Ya sea por teléfono o mensajes a través de WhatsApp, SMS, correo electrónico, chat o redes sociales, independientemente de cómo te hayan contactado.

Siempre que sea posible, averigua quién es tu gerente personal y ten en cuenta que nunca te pedirán que retires dinero de tu cuenta.

Fraude falso videollamada

En Itaú, no hacemos videollamadas sin tu consentimiento, ni solicitamos que muestres la pantalla del cajero automático cuando estés allí.

En Itaú, no hacemos videollamadas sin tu consentimiento, ni solicitamos que muestres la pantalla del cajero automático cuando estés allí.

¿De qué se trata?

Muchos estafadores practican estafas a través de videollamadas. En este tipo de acciones suelen llamar e identificarse como funcionarios del banco, ofreciendo ayuda a los clientes que están pendientes del lanzamiento de Token
o con otras dificultades en tu cuenta. La mayoría de las veces aceptan ponerse en contacto contigo para poder ayudarte cuando estés en el cajero automático.

¿Cómo puedes evitarlo?

Nunca envíes videos, fotos y/o capturas de pantalla del cajero automático, ni muestres la pantalla mediante una videollamada cuando esté allí.

Fraude falso Contact Center

No escribas tu contraseña en el teclado del teléfono o proporciones tus datos en las llamadas que recibas.

Elige llamar al Contact Center a través de un teléfono celular y proporciona tus datos solo en esas llamadas directas.

¿De qué se trata?

Una persona (el estafador) te llama y se identifica como funcionario del banco Itaú del Contact Center. El propósito del fraude es obtener tu contraseña y datos personales, además de los números de tarjeta, códigos de seguridad y códigos Token.

¿Cómo pasa?

Este tipo de fraudes generalmente ocurren cuando:

1. El defraudador te llama al teléfono fijo, a nombre de Itaú, y te dice que se han realizado compras con tu tarjeta debido de altos valores, dice que necesita tu confirmación. Como son compras inventadas, dices que no las realizaste.

2. El defraudador informa que se trata de un posible fraude y te indica que realices una llamada al Contact Center, marcando el número impreso en el reverso de la tarjeta, para regularizar la situación.

3. Ahí es cuando ocurre la estafa, sin que te des cuenta, el estafador finge colgar, pero permanece en la línea, por lo que se obstruye la llamada.

Puede oírte llamar a la central y cuando respondes, crees que estás hablando con nuestro Contact Center, ya que se simulan varios aspectos del Contact Center real, como la música, los mensajes e incluso el propio menú de servicio;

4. Con todo esto, crees que estás en contacto legítimo con el banco y terminas transmitiendo al estafador datos, como códigos de seguridad, códigos Token y número de tarjetas, además de ingresar la contraseña en el teclado del teléfono.

¿Cómo puedes evitarlo?

Nunca ingreses tus contraseñas en el teclado del teléfono ni brindes ningún otro dato personal a quien te llamó en nombre de Itaú, especialmente en el teléfono fijo.

Siempre trata de comunicarte con el Contact Center desde un teléfono celular. Si te dan un número de teléfono para llamar, consulta el sitio web oficial de Itaú para ver si el número es legítimo.

Fraude por WhatsApp

Fraude por WhatsApp

No compartas los códigos de verificación que recibes por SMS en las llamadas o por chat.

Sospecha cuando te soliciten contraseñas, códigos de confirmación o datos personales a través de WhatsApp o por teléfono.

¿De qué se trata?

La estafa de WhatsApp es una de las más recurrentes en la actualidad. En este tipo de fraudes, el objetivo principal es acceder a la lista de contactos de la víctima, para que el estafador pueda hacerse pasar por él y pedir dinero a amigos cercanos.

¿Cómo pasa?

Este es el paso a paso del defraudador para aplicar esta estafa:

1. Identifica tu número de teléfono celular.

2. En cualquier teléfono celular, instala WhatsApp y usa tu número de registro.

3. Después de eso, te llamará pretendiendo ser de cualquier empresa con la que tengas una relación.

4. Durante la conversación, dice que recibirás un SMS con un código, el cual debe ser informado para confirmar algunos datos o para confirmar o continuar el contacto.

5. Este código libera tu cuenta de WhatsApp en el teléfono celular del estafador. Con este comunicado, podrá hacerse pasar por ti y, mediante el intercambio de mensajes, conseguir que tus contactos más cercanos transfieran dinero a su cuenta o informen datos confidenciales.

¿Cómo puedes evitarlo?

Nunca ingreses tus contraseñas, códigos de confirmación o datos personales en las llamadas y mensajes que recibas. Ningún empleado de Itaú solicitará esta información a través de WhatsApp o por teléfono.

Para estar siempre seguro, activa la verificación de 2 pasos en WhatsApp, que es la función de protección propia de una aplicación contra el fraude. Ve a: Configuración> Cuenta> activa la "Verificación en 2 pasos"> Registra una contraseña. La contraseña debe ser memorizada, ya que la aplicación le indicará de vez en cuando durante su uso y siempre que inicies sesión en tu cuenta en otro dispositivo móvil o computadora (WhatsApp Web).

Fraude de phishing

(Busca robar tu información)

Fraude bloqueo de cuenta

En Itaú, no enviamos mensajes de correo electrónico, SMS o WhatsApp para informar que tu cuenta se bloqueará por algún motivo, como, por ejemplo, actualización de información.

Presta mucha atención a los mensajes recibidos por correo electrónico o mensaje de texto.

¿De qué se trata?

Las estafas por correo electrónico están diseñadas para identificar tus contraseñas y robar información personal y bancaria, como los códigos de Token, los números de tarjeta y códigos de validez y seguridad.

Incluso, pueden instalar programas maliciosos en tu computador sin que te des cuenta. Uno de los argumentos más utilizados por los estafadores en esta modalidad es advertir que tu cuenta será bloqueada, por ejemplo, porque no has actualizado tu registro o tu clave no coincide.

¿Cómo pasa?

En la estafa del falso correo electrónico sobre el bloqueo de la cuenta. Recibes un correo electrónico en nombre del banco en el que se te informa de posibles irregularidades en tu registro, o incluso de la falta de actualización del mismo, lo que puede llevar a que tu cuenta sea bloqueada completamente.

El contenido de estos correos electrónicos suele tener estas características:

- Información sobre el posible bloqueo de la cuenta, debido a un registro desactualizado.

- Con un enlace solicita el clic inmediato, para que hagas la regularización y la cuenta no se bloquee.

- Solicita directamente contraseñas, códigos o validación del Token e información personal para evitar que la cuenta sea bloqueada.

¿Cómo puedes evitarlo?

Ten presente que Itaú nunca solicita información como contraseñas, Token o códigos de validación, y mucho menos números de tarjeta y CVV en los correos electrónicos o mensajes que envía.

Nunca hagas clic en los enlaces para actualizar tu registro o descargar cualquier tipo de programa o archivo para evitar que tu cuenta sea bloqueada. Acciones como estas no solo ponen en riesgo tus datos, sino que también pueden dañar tus dispositivos electrónicos

Fraude por actualización O sincronización de token PJ

Itaú no te envía correos electrónicos, SMS o WhatsApp para informarte de que tu Token se bloqueará por falta de actualización o sincronización.

Cuando tengas alguna pregunta, por favor llámanos directamente desde un teléfono móvil.

¿De qué se trata?

La estafa por actualización o sincronización de Token tiene como objetivo robar el código del Token que usas en tus validaciones. Uno de los argumentos utilizados en esta estafa es el bloqueo del código de tu Token, debido a la falta de actualización o sincronización.

¿Cómo pasa?

Recibes un correo electrónico o un SMS con un enlace, en nombre del banco, en el que se te informa de que tu código de Token no ha sido actualizado o sincronizado, indicando que, si no actualizas o sincronizas inmediatamente tu código, será bloqueado. Además, este correo electrónico puede contener solicitudes de contraseñas e información personal. Al hacer clic en el enlace, se te dirige a una forma o página falsa. Allí, al introducir tu contraseña y los datos solicitados, será capturada por el estafador y utilizada más tarde

¿Cómo puedes evitarlo?

Siempre ten presente que Itaú nunca solicita información como contraseñas, Token o códigos de validación, y mucho menos números de tarjeta y CVV en los correos electrónicos o mensajes que envía. Recuerda que para Persona Jurídica se puede solicitar matriculación de direcciones IP, realizar restricción de horarios y días para acceso al Portal, Parametriza en el Portal por montos y transacciones de acuerdo con el volumen de negocio.

Fraude de SMS con link

No introduzcas datos personales o contraseñas a través de SMS.

Lee cuidadosamente cualquier mensaje que recibas en nombre de Itaú.

¿De qué se trata?

Es muy común que los estafadores actúen a través de SMS. En este tipo de acción, suelen enviar enlaces maliciosos para dirigir a la víctima a un formulario o página que le pedirá datos como contraseñas, códigos de seguridad o de Token, números de tarjeta, etc.

¿Cómo puedes evitarlo?

Siempre ten en cuenta que Itaú nunca solicita datos personales como contraseñas, códigos de Token o número de tarjetas por mensajes SMS. No hagas clic en los enlaces que piden el registro o la actualización de Token, ni proporciones ningún tipo de información por mensaje. En caso de duda, ponte en contacto con nosotros a través de los canales oficiales informados en la página oficial del banco.

Fraude por robo de información

Itaú no envía mensajes de correo electrónico con link para acceder a la página del Banco.

Debes mantener actualizado el antivirus, el navegador y el sistema operativo de tus dispositivos electrónicos.

¿De qué se trata?

La estafa inicia con la instalación de un virus u otros programas maliciosos en tus equipos electrónicos, el estafador envía un e-mail falso con asunto polémico para que sientas curiosidad y hagas clic en los links. Ignora los correos electrónicos en los que te ofrezcan premios o soliciten datos personales o financieros.

Este tipo de fraudes generalmente ocurren en los siguientes escenarios:

1. Infección de computador

   Para acceder a tu cuenta por Internet, necesitas escribir tus datos. Previamente, será necesario saber si tu computadora está infectada.

   La infección sucede cuando el usuario hace clic en links dudosos, abre archivos anexos o ejecuta programas anexados tipo ".exe", ".scr" o ".zip" recibidos por e-mail. Es en este momento que un programa espía es instalado y se establece el primer contacto con el estafador.

2. Obtención de la información

Después de infectar tu computador, este pasa a ser monitoreado por el estafador sin que tú lo sepas. Así, es posible obtener tus datos de dos formas:

A. Te envía a un sitio falso, muy parecido al de tu banco. En este sitio falso, son solicitados datos personales como número de documento, cuenta y contraseñas del banco, si las introduces, estás entregando tu información al estafador.

B. Otra manera de obtener datos ocurre cuando accedes al sitio verdadero del banco y un programa malicioso instalado en tu computador, comúnmente llamado troyano, guarda las teclas digitadas y envía tu información al estafador. De esta forma podrá obtener tus datos personales.

3. El hecho del fraude ocurre cuando el estafador conoce tus datos y puede realizar transacciones bancarias en tu nombre, transferencias ACH, Pagos PSE, sin que tú lo sepas.

4. Malware: Es un término que abarca cualquier tipo de software malicioso diseñado para dañar o explotar cualquier dispositivo, servicio o red programable. Los delincuentes cibernéticos generalmente lo usan para extraer datos que pueden utilizar como chantaje hacia las víctimas para obtener ganancias financieras.

¿Cómo puedes evitarlo?

Nunca ingreses por medio de mensajes de correo electrónico con link para acceder a la página del Banco. En caso de duda, ponte en contacto con nosotros a través de los canales oficiales informados en la página oficial del banco.

Recuerda mantener actualizado el sistema operativo de tus dispositivos.

Adicionalmente, recomendamos entrar a la tienda (Google play para Android o AppStore para iOS), hacer una búsqueda por “antimalware” y escoger el de tu preferencia.

Tips de seguridad de la información y Ciberseguridad

Seguridad en correos electrónicos y phishing

- Desconfía de correos con mensajes alarmantes.
- No abras archivos con adjuntos de correos sospechosos.
- Evita abrir correos de remitentes desconocidos.
- No compartas tus datos personales ni información financiera.
- Utiliza un antivirus seguro para protegerte de mensajes maliciosos.
- No compartas tus claves personales.
- Nunca hagas clic en vínculos de correos desconocidos.

Ingeniería Social
Prevención de Fraude

Recuerda que los ataques informáticos buscan tener y robar información como:

1. Datos personales
2. Información financiera
3. Credenciales de acceso

Los medios más usados para robar esta información son:

1. Redes sociales
2. Correo electrónico
3. Llamadas telefónicas
4. Mensajes de texto

Ten presente estos tips, así evitarás ser víctima de ataques informáticos.

I. Revisa si el mensaje proviene de una persona o entidad que conozcas.

II. Asegúrate de la confiabilidad del remitente:
   - Que el nombre y la dirección de correo del remitente estén bien escritos.
   - Verificar la identidad por canales oficiales.

III. Nunca realices las acciones que te pidan:
   - Hacer clic.
   - Responder el mensaje.
   - Dar información personal, etc.

ú nunca te solicita información, Token o clave por ningún adas, SMS, correo o WhatsApp).

s un caso sospechoso o eres víctima de un ataque cibernético, talo al correo: ciberseguridad@itau.co

Seguridad web

Recuerda: nunca te llamaremos para pedirte claves de acceso a internet, de Token o preguntas secretas de confirmación.

Si alguien te solicita esa información, ¡cuelga!

Mantén la seguridad de nuestros productos bancarios.

1. Descarga apps e información de plataformas verificadas.
2. Evita compartir información en sitios dudosos.
3. Actualiza constantemente tus contraseñas.
4. Monitorea lo que hacen tus hijos cuando estén navegando.

Seguridad
Productos bancarios

Estás en riesgo si respondes afirmativamente a uno o más de las siguientes preguntas:

- ¿Te ha llegado una llamada o mensaje sospechoso?
- ¿Has compartido claves bancarias a través de llamadas?
- ¿Te han pedido dinero por adelantado por parte de tu banco?
- ¿Has compartido noticias financieras sin verificar fuentes?
- ¿Tu línea telefónica se ha bloqueado misteriosamente?
- ¿Te ha llamado un familiar a pedirte dinero resultado en una situación de robo?

¡Recuerda!

Juntos podemos prevenir el fraude y suplantación de identidad en procesos bancarios:

- Evita compartir información personal por llamadas. Tu banco ya posee esa información y la puede corroborar.
- Reporta si tu línea de celular se encuentra fuera de servicio y no lo has solicitado, llama al banco y a tu operador para verificar.
- Denuncia si eres víctima de un ataque cibernético.

Canales de denuncia:

Para reportar fraudes comunícate:

Armenia	*745 1700*	*Manizales*	*887 9818*
Barrancabermeja	*611 7786*	*Medellín*	*604 1818*
Barranquilla	*385 1818*	*Montería*	*782 3823*
Bogotá	*581 8181*	*Pasto*	*723 5120*
Bucaramanga	*697 1818*	*Pereira*	*340 1818*
Cali	*486 1818*	*Popayan*	*823 0333*
Cartagena	*693 1818*	*Tuja*	*740 2126*
Cúcuta	*571 3190*	*Villavicencio*	*662 6460*
Ibagué	*263 0789*	*Resto del Pais*	*01 8000 512 633*

Comunicación sospechosa

seg_infor@itau.co

ciberseguridad@itau.co

Comparte esta información
con tus familiares y amigos.