CONSEJOS DE SEGURIDAD

RECOMENDACIONES PARA EVITAR ESTAFAS Y PROTEGER TUS DATOS.

BANCOPIANO

BANCOPIANO

PRINCIPALES RECOMENDACIONES

¿Qué hacer si sufriste una estafa o sospechás de una?

En caso de que hayas sufrido un fraude, percibís que podés ser víctima de uno o hubo un uso indebido de tus claves, **mantené la calma y bloqueá los accesos a tus cuentas bancarias.**

¿Cómo bloquear los accesos a tu cuenta de Banco Piano?

1. Comunicate a nuestro **Centro de Atención Telefónica: 0810-122-2770**, opción **3** y luego **5** o llamá a **Red Link**: **4319-LINK** (5465), opción **2**.

2. Respondé las preguntas que te realice el operador para **validar tu identidad**.

   Una vez validos tus datos, el operador gestionará el **bloqueo para resguardar tu cuenta.**

¿Cuáles son los horarios de atención?

Centro de Atención Telefónica: de lunes a viernes, de 9 a 17 horas.

Red Link: los 365 días del año, las 24 horas.

BANCOPIANO

Consejos a tener en cuenta para cuidarte de este tipo de estafas y proteger tus dispositivos.

No compartas tus claves ni datos personales. El banco no te pedirá tus usuarios, contraseñas o número de tarjeta. Esta información es **personal y confidencial**.

Ingresá al sitio web del banco de manera segura, tipeando la dirección oficial: **www.bancopiano.com.ar.**

Evitá hacer clic en enlaces sospechosos. Tené en cuenta que los sitios web son seguros si contienen en su barra de dirección la sigla **HTTPS** y la imagen de un **candado cerrado.**

Al usar tu tarjeta para pagar en comercios, **evitá perderla de vista**.

No compartas tu clave **Token**. Este **código es personal** y te sirve para autorizar operaciones por Home Banking.

Al contactarnos por **Facebook**, hacelo a nuestro **perfil oficial**: **@BancoPianoArg** y procurá **enviarnos un mensaje privado** para evitar que posibles estafadores te contacten en nuestro nombre. Además, es importante no brindar información sensible de manera pública en el muro.

Si tu celular se quedó sin cobertura, **contactá de inmediato a tu empresa** proveedora del servicio para conocer el motivo.

Destruí los documentos que tengan información personal como recibos, resúmenes o comprobantes **antes de ser descartados a la basura**.

No ingreses a **plataformas desconocidas** ni realices **pagos o transferencias** indicadas por llamadas telefónicas.

BANCOPIANO

Mantené actualizados tus sistemas operativos y **aplicaciones** para beneficiarte de las mejoras de seguridad.

Asegurate de tener el **firewall activado y un antivirus actualizado** en tu pc.

Es preferible que no utilices redes wifi públicas al llevar a cabo tus **operaciones financieras.**

Si usas una pc compartida, utilizá la funcionalidad de **teclado virtual** y asegurate de **cerrar la sesión** cuando finalices tus operaciones online.

Descargá software y aplicaciones solo de **sitios web de confianza** y verificá siempre su autenticidad para **evitar que un virus infecte tu pc.**

Asegurate de tener configuradas **opciones de bloqueo,** como contraseñas, patrones, PIN, reconocimiento facial o de huellas dactilares.

Revisá regularmente los **permisos de las aplicaciones** que tenés instaladas. Si una aplicación solicita permisos que no parecen necesarios para su funcionamiento, considera la posibilidad de desinstalarla.

En caso de **pérdida o robo**, asegurate de tener configurada la opción de **borrado remoto**. Esto te permitirá borrar todos los datos de tu dispositivo a distancia.

Tené en cuenta que tu **número de teléfono** puede ser una pieza de **información sensible**, por eso intentá limitar la cantidad de lugares en los que compartís ese dato.

BANCOPIANO

TIPOS DE ESTAFAS

Estafas físicas:
se trata de la clonación, copia, robo de datos de las tarjetas y/o captura de tu dinero, a través de cajeros automáticos o compras en comercios.

¿Cuáles son las principales estafas físicas?

SKIMMING (clonación de tarjetas)

El Skimming es el robo de información de tu tarjeta que puede hacerse mediante cajeros automáticos o transacciones en comercios a través de las terminales electrónicas de pago adulteradas (ej: Posnet).
Una vez que los estafadores tienen tu información, la utilizan para realizar compras online o bien, volcar tus datos en una nueva tarjeta en blanco.
En cajeros automáticos se realiza de distintas maneras. Por ejemplo:

- ranuras falsas instaladas donde se inserta la tarjeta y lectores adulterados de ingreso a los recintos para copiar los datos
- microcámaras ubicadas en la parte superior del cajero para leer las claves privadas
- teclados superpuestos que replican las teclas presionadas

En comercios se utilizan principalmente:

- aparatos clonadores de información que caben en un bolsillo de pantalón o palma de la mano de los estafadores y los utilizan para copiar tus datos. En este caso no lo notarás ya que pueden esconderlos y utilizarlos tras un mostrador o mientras caminan hacia la caja.

CASH TRAPPING (captura de efectivo)

Se trata de una estafa cada vez más habitual mediante la cual los estafadores se quedan con tu dinero en efectivo. Para eso, bloquean la salida de los billetes en los cajeros automáticos, a través de piezas camufladas en la ranura de los mismos. De esa forma, simulan que el dinero no se dispensó y que hubo un error en el sistema del cajero. Al retirarte del recinto, pensado que la terminal no funciona de manera correcta, ellos proceden a destrabar la ranura y retirar tu dinero.

¿Cómo evitar las estafas físicas?

- Al utilizar un cajero automático verificá que no posea algún tipo de elemento extraño o se encuentre vandalizado.
- Al introducir tu clave PIN en un cajero automático o al realizar una compra en comercios, evitá que la misma sea vista por terceros. Si es posible, tapala con tu otra mano o con algún elemento al momento de tipearla.
- Cuando entregues tu tarjeta en un comercio, evitá perderla de vista.
- Cuando pagues con tarjeta en un restaurante, solicitá que te acerquen el dispositivo de cobro a la mesa, o bien, dirigite a la caja.
- Utilizá cajeros automáticos que se encuentren bien iluminados y preferentemente en sucursales bancarias. Si es posible, evitá aquellos que se encuentran en centros comerciales dado que tienen mayor exposición.
- Controlá con frecuencia los movimientos de tu cuenta bancaria.
- Si sospechás que tus datos fueron vulnerados comunicate con nosotros al: 0810-122-2770 y con la Red Link: 4319- LINK (5465).

BANCOPIANO

Estafas virtuales:
consisten en sustraer datos personales a través de medios electrónicos como: e-mails, redes sociales y sitios web falsos para, generalmente, acceder a tus cuentas bancarias y robar tu dinero.

¿Cuáles son las principales estafas virtuales?

SIM SWAPPING (duplicado de tarjeta SIM)

Este tipo de estafa se basa en duplicar la tarjeta SIM de tu celular. Para eso, los estafadores se contactan con las empresas proveedoras de servicio de telefonía y, a través de técnicas de ingeniería social (persuasión), consiguen la información de tu SIM. Luego, con esos datos logran, entre otras acciones:

- acceder a los perfiles de tus contactos
- alterar el segundo factor de autenticación de las App
- obtener datos de tu cuenta bancaria

Solo se necesita una serie de tus datos personales para obtener un duplicado de la tarjeta SIM. Por eso, es importante que no divulgues información personal en redes sociales o portales públicos.

PHISHING (suplantación de identidad)

Para lograr este fraude de suplantación de identidad, los estafadores te contactan haciéndose pasar por entidades oficiales mediante: e-mail, redes sociales, SMS o llamadas telefónicas con el propósito de obtener tus claves de acceso a Home Banking, cuentas bancarias, números de tarjeta, etc.

Para eso, seleccionan la entidad/empresa a la que van a suplantar, determinan qué información personal tuya necesitan, eligen el medio a través del cual te van a contactar y crean un mensaje que suele ser alarmista para provocar que reacciones de manera inmediata, generalmente, logrando que hagas click en un enlace falso o bien, logrando que descargues una App fraudulenta.

Tené en cuenta que al realizar alguna de estas acciones que te piden los estafadores, estás ingresando a un sitio web suplantado o a una App falsa mediante los cuales capturan tus datos y los almacenan en un servidor remoto controlado por ellos que les sirve para robar tu dinero y generar nuevas estafas a tu nombre.

PHARMING (redirección a sitios web falsos)

En este tipo de engaño sobre sitios web, los estafadores primero logran vulnerar la seguridad de tu dispositivo apoderándose de él y buscan direccionar tu navegación hacia un sitio web falso creado de manera fraudulenta para obtener tus datos personales y/o bancarios. Generalmente, los estafadores suelen centrar sus ataques a través de sitios falsos del sector financiero, plataformas de pago y similares.

VISHING (contacto de entidades falsas)

El vishing es un engaño a personas por medio de llamadas telefónicas para robar información personal y bancaria. Para estos casos los estafadores primero obtienen tu información personal (nombre, apellido, e-mail, datos de tarjetas, etc.), a través de otros métodos, como el Phishing. Con esta información, se contactan por llamadas o mensajes simulando ser entidades bancarias o empresas de servicios y, abusando de la confianza que se genera por el conocimiento de datos sensibles durante la conversación, logran engañarte para que les realices transferencias de dinero o instalan virus en tus dispositivos.

REDES SOCIALES (perfiles falsos)

En estos casos, la base del fraude es también la suplantación de identidad de empresas / entidades oficiales para obtener tus datos y dinero. Es así que los estafadores crean perfiles falsos de entidades y responden tus consultas mediante grupos o cuentas en Facebook y otras redes sociales con la excusa de ayudarte y orientarte. De esta forma, te derivan a sitios web fraudulentos o te solicitan datos privados para acceder a tus cuentas bancarias.

VIRUS A TRAVÉS DE E-MAILS (archivos adjuntos)

Para lograr esta estafa que tiene como fin instalar virus en tus dispositivos, los ciberdelicuentes te envían un correo electrónico con un archivo adjunto -que contiene escondido un virus- , por lo general es en formato comprimido (ej: .zip). En caso de que abras este archivo, el virus se instalará en tu dispositivo y cuando ingreses a un sitio bancario o Home Banking, los estafadores podrán tener acceso a tus datos personales y, por tanto, realizar todo tipo de movimientos en tu cuenta.

MALWARE (virus informático)

El malware es un tipo de virus informático que se propaga mediante programas o intercambio de archivos, con el fin de alterar el funcionamiento normal de tu computadora o celular. De esta manera, los estafadores logran obtener tus datos personales e información privada de tus dispositivos.

BANCOPIANO

¿Cómo evitar las estafas virtuales?

- Si alguien de tus contactos te escribe por WhatsApp para pedirte dinero, primero busca otro medio alternativo para validar que el pedido sea genuino antes de realizar una transferencia.
- De ningún modo reenvíes códigos de seguridad que recibas por WhatsApp, SMS o email.
- Desde el banco no te vamos a pedirte telefónicamente que devuelvas una transferencia recibida en tu cuenta, ni te solicitaremos que actives un préstamo para generar esa devolución.
- Si te ofrecen premios, verificá que sean legítimos a través de la entidad/empresa oficial. Los estafadores intentarán captar tu atención con promociones o condiciones demasiado atractivas para que facilites datos personales por miedo a perder la oportunidad de ganar.
- Evita abrir archivos adjuntos o links que recibas por e-mail de remitentes desconocidos.
- Si interactúas en redes sociales, hacelo con perfiles oficiales y no divulgues información personal de manera pública.
- Ante cualquier duda, siempre comunícate con nuestros canales oficiales.

¡Recordá estos consejos para proteger tus datos y operar de manera segura!

Si sospechás que tus datos fueron vulnerados, comunicate con con nosotros:
Centro de Atención Telefónica: 0810-122-2770
Denuncias Red Link: 4319-5465

BANCOPIANO

CONOCÉ NUESTROS CANALES OFICIALES DE ATENCIÓN:

TELÉFONO
0810-122-2770

SITIO WEB
www.bancopiano.com.ar

E-MAIL
info@piano.com.ar

REDES SOCIALES
Facebook: @BancoPianoArg

MÁS INFORMACIÓN

Protección al usuario financiero:
www.usuariosfinancieros.gob.ar

Teléfonos útiles:
Centro de Atención Telefónica **0810-122-2770**
Red Link **4319-LINK (5465)**