CONSEJOS DE SEGURIDAD

La tecnología está evolucionando de manera acelerada y cada día es más compleja. Esto propicia la aparición de nuevos y más frecuentes riesgos para la seguridad de la información. Como consecuencia, la seguridad de la información y la ciberseguridad está en las agendas de los principales organismos y empresas, es por ello que Banco Sabadell se ha puesto como principal objetivo proteger su información y la de sus clientes a través de mecanismos robustos de Seguridad.

Banco Sabadell le presenta los consejos de seguridad que usted debe saber para evitar ser víctima de un fraude:

SEGURIDAD EN SERVICIOS DE BANCA EN LÍNEA

- Cuando navegue por Internet y/o reciba correos electrónicos es conveniente que no introduzca datos sensibles relacionados con usted o su cuenta de acceso a la banca en línea y principalmente:
  - En las páginas a las que haya accedido a través de un correo electrónico.
  - En los correos electrónicos que usted envíe, ni siquiera en el caso de que se lo solicite alguien en nombre del Banco.
  - En caso de que dude de la autenticidad de la página web en la que se encuentra.
- Al generar sus claves de acceso, le sugerimos utilizar combinaciones de números y letras mayúsculas y minúsculas. No utilice datos predecibles o de posible conocimiento público como: nombres de familiares, RFC, CURP, teléfonos, fechas de cumpleaños, tu número de cuenta, etc.
- Cuide no dejar desatendida la computadora cuando se encuentre conectado a nuestra banca en línea.
- Evite acceder a su banca en línea desde equipos públicos como de cibercafés, hoteles, etc.
- Evite acceder a su banca en línea desde redes públicas desprotegidas.
- Evite ser observado al digitar sus contraseñas, especialmente al utilizar el servicio en lugares públicos; si esto sucede, le sugerimos cambiar sus claves lo más pronto posible.
- Le informamos que desde Banco Sabadell nunca le pediremos datos confidenciales, como contraseñas o números de cuenta, ni por correo electrónico, ni telefónicamente.

SEGURIDAD EN SERVICIOS DE BANCA MÓVIL

- Cuidado con las apps que descargue, instale únicamente aquellas aplicaciones que estén disponibles en los mercados de descarga oficiales de los dispositivos (Ej: Google Play, App Store, etc).
- Compruebe que las aplicaciones para móvil vengan de desarrolladores confiables, las opiniones de otros usuarios también nos pueden ayudar a discernir.
- No aplique “jailbreak” al dispositivo móvil que utilice para acceder a su Banca Móvil.
- Utilice la aplicación oficial de Banca Móvil. Una forma de asegurarse de que estamos descargando la aplicación correcta es visitando la página web de Banco Sabadell desde el móvil y saltará un mensaje preguntando si la queremos descargar con un enlace a los mercados de descarga del dispositivo en cuestión.
- Mantenga todo el software, tanto sistema operativo del dispositivo como las aplicaciones descargadas, actualizado a la última versión disponible.
- No pierda de vista el dispositivo móvil para evitar su robo, así como la posible manipulación malintencionada de las aplicaciones instaladas en éste.
- Utilice un código de al menos 6 dígitos para acceder a su dispositivo móvil, o bien si este lo permite haga uso del identificador de huellas para incrementar el nivel de Seguridad.
- No haga uso de operaciones de banca cuando se encuentre en una red pública desprotegida.
- No almacene datos bancarios en el celular (usuario, código acceso, etc.)

- Habilite mecanismos de bloqueo de pantalla y active, si se dispone, un sistema antirrobo.
- Bloquee el dispositivo móvil cuando este no se encuentre en uso.
- Si pierde o le es robado su dispositivo móvil, no olvide en cambiar sus contraseñas de acceso a la Banca Móvil y en caso de ser posible realice un borrado remoto del mismo.

SEGURIDAD PARA EL USO DE SU TARJETA DE CRÉDITO SABADELL

- Usted recibirá su tarjeta de crédito en una bolsa de seguridad, asegúrese de que ésta no haya sido abierta y que cumpla con las medidas de protección señaladas en la misma.
- Al recibir su tarjeta es importante firmarla de forma inmediata.
- Si su tarjeta venció, se deterioró o la canceló, destrúyala raspando la firma y cortando el plástico en fragmentos o introduciéndola en una trituradora de papel que también admita destrucción de tarjetas.
- No preste su tarjeta, ni permita que otras personas la usen en su nombre.
- Su NIP llegará por separado, destruya el documento y preferentemente memorice el número, pero si no le es posible y necesita anotarlo, guárdelo en un lugar realmente seguro. Recuerde que este número es exclusivo para operaciones en cajeros automáticos (ATMs).
- Cambie el NIP frecuentemente, y siempre que alguien más lo pueda saber, y evite utilizar números fácilmente identificables como cumpleaños, etc.
- No permita asesoría de extraños ni permita que observen su NIP al digitarlo en cajeros automáticos (ATMs).
- Al retirarse del cajero automático (ATMs) no olvide llevar su tarjeta.
- Al pagar con su tarjeta en establecimientos comerciales y restaurantes procure no perder de vista su tarjeta o solicite que la terminal punto de venta (TPV) sea llevada hasta su lugar. Cuando se la devuelvan verifique que sea su tarjeta.
- Al realizar compras por internet, hágalo en comercios que garanticen la confidencialidad de sus datos personales y de su tarjeta con algún certificado de seguridad.
- Durante sus viajes, nunca deje sus tarjetas en la habitación, ni aún guardadas dentro de una maleta. Procure dejarlas en la caja de seguridad del hotel.
- No crea en las promesas de regalos o premios y/o cualquier otro argumento para obtener su información vía telefónica, en mensajes de texto o por correo electrónico.
- Concilie oportunamente los movimientos que aparecen en su estado de cuenta. En caso de que haya inconsistencias repórtelo al Centro de Atención Telefónica.
- Eventualmente podría recibir llamadas del Centro de Atención Telefónica para verificar si realizó transacciones diferentes a su patrón de comportamiento, atienda las mismas tan pronto le sea posible.
- En caso de robo o extravío de su tarjeta de crédito, repórtelo de inmediato al Centro de Atención Telefónica: **01 800 1102 200.**

CONSEJOS SOBRE SEGURIDAD EN SUS EQUIPOS DE CÓMPUTO, TABLETS Y/O SMARTPHONES

Para prevenir posibles problemas de seguridad derivados de las vulnerabilidades que se descubren ocasionalmente en el software utilizado en los equipos de cómputo, es conveniente visitar las páginas de seguridad de los fabricantes de los programas que utilizamos, en especial el navegador y el propio sistema operativo.

- Verifique la existencia de actualizaciones del sistema, incluyendo actualizaciones de seguridad.
- Realice copias de seguridad de forma regular con el objetivo de poder recuperar la información disponible en su equipo de cómputo, tablet o smartphone con anterioridad a la existencia de algún problema en el mismo.
- Utilice software, servicios y sitios de Internet de confianza.
- Le recomendamos que se abstenga de ejecutar programas que le lleguen por correo electrónico, aunque su origen parezca conocido, cuando no esté totalmente seguro de su procedencia

- No confiar en certificados presentados durante la navegación sin verificar previamente su origen.
- Preferiblemente use redes wifi confiables y seguras para conectarse con Banca por internet o Banca Móvil.
- Para los equipos de cómputo utilice un sistema antivirus, fortaleciéndolo con otro tipo de herramientas de seguridad como firewalls personales, detectores de intrusos y manténgalos permanentemente actualizados.

Le aconsejamos tomar las debidas precauciones y desconfíe de comunicaciones no habituales o sospechosas, en las que se le requiera información confidencial, se informe del bloqueo de su cuenta o se requiera de una acción por su parte que pueda suponer un movimiento de fondos.

En caso de que usted detecte o sospeche de una posible acción de fraude electrónico o cualquier anomalía, contáctenos a los teléfonos:

- Centro de Atención Telefónica: **01 800 1102 200**
- Banco Sabadell: **(52) 55 52623200**

Y a través del servicio de oficina telefónica mantendremos la comunicación con usted durante el período de resolución de la incidencia para cualquier tipo de consulta y notificación.

Así mismo, en el caso que Banco Sabadell detecte operaciones potencialmente fraudulentas, se pondrá en contacto con usted mediante el servicio de oficina telefónica para determinar la legitimidad de la operación y establecer los próximos pasos necesarios, siempre con el objetivo de ayudarle y protegerle ante actividades ilícitas. Con esa finalidad, Banco Sabadell actualizará periódicamente este apartado de seguridad para prevenirle de posibles intentos de fraude que puedan ser empleados.