

Aspectos referidos a la seguridad en el uso del Home Banking

IMPORTANTE: Le recordamos 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.). Banco de Comercio S.A. en ningún caso se comunicará con Ud. requiriéndole este tipo de información. En caso de encontrarse en una situación similar a las descriptas anteriormente comuníquese con la casilla de correo soportehb@bancodecomercio.com.ar

Seguridad en Internet:

Banco de Comercio S.A. utiliza los más altos estándares y normas de seguridad en Internet para garantizar la confidencialidad e integridad de los datos. Todas las aplicaciones de nuestra arquitectura son regularmente testeadas y controladas para que los sistemas puestos a su disposición sean seguros y usted pueda operar con total confianza y seguridad. Para garantizar su privacidad al acceder a nuestra página, Banco de Comercio S.A. pone a su disposición las siguientes medidas de control.

Identificación del sitio:

Para comprobar que se está conectando con el sitio correcto en la página de acceso a la Banca Internet (Home Banking) podrá comprobar que, en la parte izquierda o derecha, dependiendo el navegador que utilice, aparece un candado, el cual le informa que el sitio utiliza un canal seguro.

Certificado Digital:

La arquitectura de Banco de Comercio S.A. cuenta con el certificado emitido por Sectigo RSA Domain Validation Secure Server CA – Sectigo Limited – 18/09/2022. Este certificado garantiza que realmente se ha conectado con Banco de Comercio S.A. y que los datos transmitidos son cifrados.

Bloqueo de Claves

Como una medida adicional de seguridad, el sistema controla la cantidad de accesos incorrectos y en caso de superar 3 intentos fallidos se procederá a bloquear las mismas.

Verificación de la fecha y hora de la última conexión exitosa

Al ingresar al Home Banking con su usuario y clave, debajo de su foto de Perfil, usted podrá visualizar la fecha y hora de su último acceso exitoso al sitio web del Banco.

Desconexión Automática por inactividad

Si transcurre un lapso de (2 minutos) en el que en su dispositivo (computador, celular o Tablet, etc) permanece inactiva una sesión de Banca Internet (Home Banking), se producirá automáticamente una desconexión de la misma apareciendo en la pantalla principal del ingreso.

Segundo Factor de Autenticación

El Segundo Factor de Autenticación aplica para algunas operaciones en particular. El objetivo del Segundo Factor es permitirle que opere cómodamente en Home Banking (Banca internet y Banca móvil) sin correr riesgos de seguridad. Existen dos tipos de Segundo Factor:

- Envío SMS o Email o
- Soft token

SMS o Email:

se trata de una funcionalidad disponible para generación y obtención de claves dinámicas, las cuales serán requeridas en las distintas transacciones, en Home Banking (Banca internet). Esta opción se encuentra disponible si el cliente tiene registrado previamente número de celular o dirección de correo personales.

Soft Token:

se trata de una aplicación móvil cuya funcionalidad es la generación de claves dinámicas, las cuales serán requeridas en las distintas transacciones, en Home Banking (Banca internet).

Consejos y Recomendaciones

Equipamiento:

Se recomienda que el equipo utilice las siguientes medidas de seguridad en sus conexiones a Internet:

- PC: preferentemente utilice firewall y antivirus actualizados.
- Navegador: utilice un navegador actualizado. Para mayor seguridad podrá modificar la configuración de su navegador de la siguiente manera: desde "Herramientas/ opciones de Internet" y seleccionando la pestaña "Seguridad" podrá establecer la configuración de seguridad en "Mediano" y desactivar la "persistencia de datos de usuario" desde la opción de configuración que ofrece dicha ventana.

También en las últimas versiones del navegador podrá activar la navegación privada la cual no guarda archivos temporales en el equipo desde "Herramientas/ Seguridad /Exploración de InPrivate" (Internet Explorer). "Opciones /Nueva ventana de incógnito (Chrome).

Para una correcta visualización de su Home Banking, por favor utilice alguno de los navegadores compatibles:

- Google Chrome
- Microsoft Edge 17

Uso de contraseñas

Las claves son nuestra llave para poder ingresar a operar sus cuentas a través de Internet. Por esta razón le recomendamos usar contraseñas diferentes para servicios sensibles.

Ponga robustez a su clave:

- Diferente: evite usar la misma clave para acceder a distintos servicios.

- Que no contenga información personal: no utilice información personal o fácil de adivinar, como nombres, fechas de nacimiento, aniversarios, etc.
- No escriba su contraseña: evite escribirlas, y si lo hace, por favor asegúrese de mantenerla en un lugar seguro.
- Frecuencia: es recomendable cambiar su contraseña frecuentemente.

Acerca de los sitios de conexión

Lugares públicos:

si bien es una característica del Home Banking su amplia posibilidad de acceso desde cualquier PC conectada a Internet, se recomienda evitar lugares públicos o PC's con múltiples operadores (cybercafés, locutorios, bibliotecas, etc).

Esta recomendación tiende a la preservación de la seguridad y confidencialidad de los datos. Si de todas maneras debiera operar desde sitios públicos, le recomendamos que con posterioridad proceda al cambio de sus claves.

Esté alerta al fraude en Internet:

Debe ser consciente que hay sitios web falsos diseñados específicamente para engañar al usuario con el objetivo de extraer su información personal. Estos sitios falsos suelen vincularse con e-mails que pretenden venir de instituciones financieras o de medios de pago. Por favor utilice siempre direcciones de sitios web conocidos.

Además, le sugerimos:

- Utilizar antivirus y actualizarlo periódicamente.
- Utilizar firewall y antispyware.
- Si se utiliza Windows, actualizar el sistema operativo cada vez que Microsoft divulgue una vulnerabilidad, o bien tener activado el sistema de actualización automática.
- No ingresar al Banco por medio de direcciones o links que se reciban por e-mail.
- No guardar la clave en e-mails ni en ningún otro tipo de archivo.
- No envíe información sensible por correo electrónico.
- Tome ciertos recaudos al momento de abrir correos electrónicos sospechosos.

Informar cualquier anomalía a la casilla soprotehb@bancodecomercio.com.ar

- Procure escribir la dirección "www.bancodecomercio.com.ar" completa en la barra de direcciones del buscador o accede a través de nuestras aplicaciones oficiales en Play Store (Android) o App Store (iOS).
- No compartas tu usuario o clave con nadie. Tu clave es personal y nadie más que vos debería saberla.

Para más información, visita nuestro sitio institucional: <https://www.bancodecomercio.com.ar>