PROTECCION DE DATOS Y SEGURIDAD INFORMATICA BANQUE HERITAGE (URUGUAY) S.A.

1. Conexión Segura

BANQUE HERITAGE cuenta con las máximas medidas de seguridad para garantizar la confidencialidad de las comunicaciones entre el Banco y nuestros usuarios. El cliente podrá verificar la autenticidad de nuestros servicios web, a través del candado que se muestra a la izquierda de nuestra URL, en la barra de direcciones. Nuestro certificado esta emitido por Thawte, en la pestaña “Detalles” encontrara toda la información acerca de las características de seguridad del mismo.

2. Seguridad de sus claves y contraseñas

Su clave de acceso al e-Banking y su Token son elementos personales y privados. Cada usuario deberá custodiarlos de forma segura. No divulgue las claves ni códigos y tome las medidas adecuadas para garantizar la seguridad de los mismos. Nadie en Banque Heritage conoce sus claves.

Modifique y actualice sus contraseñas y/o claves siguiendo las recomendaciones otorgadas por el Banco. No digite claves ni contraseñas en presencia de otras personas, aún cuando pretendan ayudarlo, ni facilite el token a terceros, ya que son de uso personal. Guarde el token en un lugar seguro y verifique periódicamente su existencia. No entregue el token a terceros.

No utilice los Instrumentos Electrónicos cuando se encuentren mensajes o situaciones de operación anormales. No responda a intentos de comunicación por medios y formas no acordados con el Banco.

En caso de extravío, hurto, robo o falsificación de los Instrumentos Electrónicos o claves o códigos, o de utilización por terceros de la información contenida en los mismos sin autorización de los Clientes, los Clientes se obligan a realizar de inmediato la correspondiente denuncia ante el domicilio del Banco. También se podrá notificar al Banco al teléfono 2 916 0177 opción 1 o enviando un correo electrónico a customersupport@heritage.com.uy.

El navegador en su PC o Smartphone podrá ofrecerle la posibilidad de guardar su contraseña. Le recomendamos que nunca guarde claves de acceso al e-banking u otras contraseñas importantes ya que quedan almacenadas en la memoria de su PC o celular y pueden quedar al alcance de otras personas que utilicen esos dispositivos.

3. Desconexíón de E-Banking

Recuerde que cada vez que finalice su sesión de e-banking deberá cerrarla con la flecha de salida que aparece arriba, a la derecha de la pantalla. De esta forma habrá finalizado de forma segura su sesión en e-banking.

Recomendaciones

- RECUERDE que el Banco nunca realizará llamadas telefónicas ni lo contactará por correo electrónico, SMS, Whatsapp o redes sociales para solicitar contraseñas, pines, números de cuentas o de tarjetas.

- NUNCA entregue contraseñas o información confidencial ante llamadas de personas que se PRESENTAN COMO FAMILIARES O PERSONAS DE SU CONOCIMIENTO y les planteen situaciones de ALARMA Y URGENCIA.

- NUNCA responda un correo electrónico que incluya links, botones o espacios para agregar datos ni haga click sobre archivos adjuntos sospechosos.

- ESTÉ ALERTA con solicitudes de pagos inesperadas o irregulares y con los cambios de cuenta, banco o razón social, país, etc. al que se instruye enviar fondos.

- ESTÉ ALERTA cuando ingrese en el sitio web del banco. Compruebe que la dirección escrita en el navegador empieza con "https", o bien, está acompañada por un ícono con forma de candado.

- ESTABLEZCA ALERTAS para las compras realizadas con sus tarjetas.

- SIEMPRE utilice contraseñas seguras. Deben contener números, letras y signos especiales, con un largo mínimo de 8 caracteres. No deben ser datos obvios como fechas de nacimiento, direcciones o nombres.

- CAMBIE frecuentemente sus contraseñas.

- SIEMPRE que reciba una llamada o contacto sospechoso, contáctenos por los canales oficiales.

- Siempre que ingrese a la página transaccional del Banco, verifique que el URL empiece por https y corresponda a la dirección web del Banco.

- Nunca acceda al sitio por medio de enlaces que le envíen por correo electrónico.

- Mantenga el token y los dispositivos de autenticación físicamente seguros y bajo control permanente.

- En la medida de lo posible, configure el firewall de la red para que permita la navegación del equipo desde donde se realizan transacciones, únicamente a los portales bancarios

4. Protección de Datos

BANQUE HERITAGE garantiza la protección de los datos de sus clientes. Es por ello que el sitio web el Banco no reconoce de modo automático ningún dato referente a la identidad de los visitantes de sus páginas. A fin de garantizar la seguridad y confidencialidad de las transacciones, para acceder al e-banking de Banque Heritage, es necesaria la previa identificación y autenticación del usuario en el sistema, pormedio de la utilización de claves de acceso y token en determinados casos.

Todos los datos sobre nuestros clientes son tratados con estricta reserva no siendo estos accesibles a terceros para finalidades distintas de aquellas para las que han sido brindados, sin el expreso consentimiento del titular de los datos.