BANQUE HERITAGE
Su banco suizo en Uruguay

Buenas prácticas de seguridad informática

Lea atentamente las siguientes recomendaciones para proteger su información financiera y prevenir fraudes.

- SIEMPRE que reciba una llamada o contacto sospechoso, contáctenos por los canales oficiales: (00598) 29160177, www.heritage.com.uy, banqueheritage@heritage.com.uy. NO RESPONDA a intentos de comunicación por medios y formas no acordados con el Banco.

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

- NO INGRESE DATOS PERSONALES en sitios utilizando enlaces que llegan por correo electrónico ya que pueden ser fraudulentos.

- NO RESPONDA A MENSAJES DE AVISO sobre supuestos errores al realizar transferencias bancarias, solicitudes de pago irregulares o cambios en los datos de la cuenta a la que se pide enviar fondos. Ante cualquier duda, siempre comuníquese telefónicamente con el Banco.

- NO BRINDE DATOS PERSONALES relacionados a cuentas (claves, pin, usuarios, token, fotocopia de CI, ni ningún tipo de dato) por mail, teléfono, redes sociales o whatsapp).

- EL CLIENTE ES EL QUE DEBE ORIGINAR LA LLAMADA AL BANCO. No acuda al cajero automático, abra la app o acceda a su e-banking si recibe una llamada supuestamente proveniente del Banco.

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

- PROTEJA SUS DISPOSITIVOS con contraseñas y en caso de disponer tecnología biométrica, actívela.

- SIEMPRE UTILICE CONTRASEÑAS SEGURAS, que contengan 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. No digite claves ni contraseñas en presencia de otras personas, aun cuando pretendan ayudar, ni facilite el token a terceros, ya que son de uso personal.

- El navegador en su PC o Smartphone podrá ofrecer la posibilidad de guardar su contraseña. NUNCA GUARDE claves de acceso al e-banking u otras contraseñas importantes ya que quedan almacenadas en la memoria de la PC o celular.

- No utilice equipos públicos o dispositivos de otras personas para acceder a sus app, redes sociales o cuentas de uso personales.

- NO USE REDES WIFI PUBLICAS para acceder a sitios que requieran de contraseñas.

- MANTENGA ACTUALIZADO el sistema operativo, el navegador y las aplicaciones de sus equipos.

- NO ACCEDA a los instrumentos electrónicos cuando vea mensajes o situaciones de operación anormales.

- Al ingresar en el sitio web del banco VERIFIQUE 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 está emitido por Thawte, en la pestaña “Detalles” encontrará toda la información acerca de las características de seguridad del mismo.

- NUNCA acceda al sitio del Banco por medio de enlaces que le envíen por correo electrónico.

- 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 la sesión en e-banking.

- LE RECOMENDAMOS ESTABLECER ALERTAS para las compras realizadas con sus tarjetas.

Ayudemos a prevenir
para operar con tranquilidad.