

Buenas prácticas de seguridad informática

Le recordamos las siguientes recomendaciones para proteger su información personal, financiera y prevenir fraudes:

ATENCIÓN: Ante el incremento de denuncias de fraudes originados en contactos telefónicos engañosos, falsos correos electrónicos, mensajes de texto de dudosa autenticidad o inclusive a través de redes sociales, le recordamos que **el Banco nunca le solicitará su contraseña** por ninguna vía de comunicación. El Banco **tampoco le pedirá ningún pago previo** al otorgamiento de productos bancarios (préstamos, tarjetas de crédito, otros).

- Ingrese a nuestro sitio web a través de la URL www.heritage.com.uy y guárdela en sus favoritos para realizar accesos posteriores. Evite ingresar accediendo a través de resultados de búsquedas en navegadores. Puede verificar la autenticidad del mismo prestando especial atención que a la izquierda de la URL de nuestro sitio web escrita en la barra de direcciones, NO EXISTA la leyenda: "No Seguro" ya sea en color gris o en color rojo. Nuestro certificado está emitido por DigiCert, y puede verificar su autenticidad siguiendo los siguientes pasos:
 - (1) Hacer clic sobre el candado o el símbolo que se encuentra a la izquierda de la URL de nuestro sitio
 - (2) Hacer clic sobre "La conexión es segura".
 - (3) Hacer clic sobre "El certificado es válido".
- SIEMPRE que reciba una llamada o contacto sospechoso, contáctenos por los canales oficiales: (00598) 2916 0177, 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, códigos de validación, 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, códigos de validación, usuarios, token, fotocopia de CI, ni ningún tipo de dato) por mail, teléfono, redes sociales o WhatsApp).
- 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.
- SIEMPRE 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, aún cuando pretendan ayudar, ni facilite el token, SoftToken o códigos de validación enviados por SMS o WhatsApp 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 su PC o celular.
- JAMÁS 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, antivirus, el navegador y las aplicaciones de sus equipos.
- DESCONFÍE de correos electrónicos que presenten archivos adjuntos, en especial con extensiones .xism, .doc, .xls o archivos .zip con contraseña. En estos casos verifique la procedencia y autenticidad del mail antes de abrir o descargar los adjuntos.
- NO ACCEDA a los instrumentos electrónicos cuando vea mensajes o situaciones de operación anormales.
- 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. Al momento de realizar el pago de las compras asegúrese tener frente a usted el POS utilizado, y verifique que los bordes del mismo estén bien sellados.
- JAMÁS ingrese su usuario y contraseña en un portal que no sea al sitio web del banco, aunque en el mismo se le indique que estos datos ingresados por usted van a ser utilizados para acceder al portal de Banque Heritage.

***Ayudemos a prevenir
para operar con tranquilidad.***