UniBank

Tu opción inteligente

Consejos de seguridad para evitar ser víctimas de fraude o robo

Preocupados por la Seguridad de nuestros clientes y usuarios: Compartimos estos consejos de seguridad para evitar ser víctimas de fraude o robo:

✓**Con Tarjetas de Débito:**

✓No brinde su tarjeta de debito a nadie.

✓No entregue o comparta su clave secreta con nadie.

✓Al realizar una compra con su tarjeta de débito no pierda de vista su tarjeta.

✓Al realizar algún tipo de transacciones en cajero automático, siempre verificar que no exista ningún tipo de objeto extraño (ranuras).

✓Observe siempre a su alrededor.

✓**En Banca en Línea**

✓El uso de las credenciales al ingresar a Banca en línea (usuario y contraseña) son de uso confidencial. No compartas tu usuario y contraseña con nadie y evita anotarlas.

✓Una vez culmines de realizar tus transacciones, asegúrate de salir o culminar la sesión de tu Banca en Línea.

✓Después de un número de intentos incorrectos de ingreso al sistema, bloqueamos el acceso de Banca en línea a tu cuenta y debemos dirigirnos al Oficial de Cuenta para restablecer el servicio.

✓Al ingresar a nuestra Banca en Línea, **https://www.unibank.com.pa/**, asegúrate que el “https” tenga la letra “s”; para mayor seguridad.

✓Verifica los estados de cuentas de las transacciones realizadas.

✓Verificar que tu computadora y tu navegador de Internet tengan instaladas las ultimas actualización de Sistema Operativo y Programas de Antivirus y mantén actualizado el navegador de Internet.

Preocupados por la Seguridad de nuestros clientes y usuarios: Compartimos estos consejos de seguridad para evitar ser víctimas de fraude o robo:

✓Por Internet

***Phishing* o suplantación de identidad** es una técnica de obtener información de forma fraudulenta.

El cibercriminal utiliza como medio de comunicación el correo electrónico o algún sistema de mensajería instantánea e incluso llamadas telefónicas presumiendo provenir de una organización legítima como un Banco, engañando así al cliente.

Pharming Pharming: El pharming constituye otra forma de fraude en línea, muy similar a su pariente, el phishing.

En lugar de depender por completo de que los usuarios hagan clic en los vínculos engañosos que se incluyen en mensajes de correo electrónico falsos, el pharming redirige a sus víctimas al sitio Web falso, incluso si escriben correctamente la dirección Web de su banco o de otro servicio en línea en el explorador de Internet

Como prevenir?

✓Ignore todo tipo de solicitud de información confidencial de datos bancarios. Unibank nunca solicita información de Clientes vía electrónica.

✓Contacte a su Banco e informe de lo ocurrido en caso de recibir correos no identificados, solicitando información bancaria.

✓**NO** hagas clic en ningún enlace o botón de un sitio web sin asegurarte de que la dirección (URL) del sitio web de la empresa sea correcta.

✓**NO** abras ni guardes archivos adjuntos de remitentes desconocidos. Si recibes un archivo adjunto que no esperabas, comunícate con el Banco para verificar el contenido.

✓Si no estás seguro del origen de una ventana emergente del navegados, **EVITA** hacer clic en los enlaces o botones que aparezcan en ella.