Fiduciaria de Occidente S.A.

¡Más seguridad para usted!

En la Fiduciaria de Occidente estamos comprometidos con la seguridad de nuestros clientes; por esta razón, tenga en cuenta las siguientes recomendaciones a la hora de realizar sus operaciones a través de nuestros canales de atención.

Oficinas Propias y/o Red Bancaria

- Realice sus operaciones directamente en las áreas de caja de las oficinas bancarias o ventanillas de atención de las oficinas de la Fiduciaria.
- No entregue sus depósitos, o documento de identificación si es requerido para la operación, a ninguna persona diferente al funcionario de caja o ventanilla de atención.
- Una vez realizada su transacción, verifique que le entreguen el soporte de la operación y que éste contenga, al menos, fecha, código de la oficina, monto de la operación, número de su encargo, visado del funcionario que lo atendió.
- No permita que personas extrañas se acerquen a la caja en el momento en que se encuentre realizando alguna transacción.
- Recuerde que nuestros funcionarios portan visible el carné de identificación como empleados de la Fiduciaria de Occidente.
- La Fiduciaria de Occidente no recibe operaciones en efectivo; estas deberán realizarse a través de la red de oficinas del Banco de Occidente.
- Nunca entregue efectivo ni documentos firmados en blanco a funcionarios de la Fiduciaria.

Portal de Internet www.fiduoccidente.com.co

- Mantenga en absoluta reserva sus claves e información financiera. No las comparta con nadie.
- Su usuario y contraseña de acceso a nuestro portal de Internet son confidenciales. La Fiduciaria de Occidente nunca le solicitará estos datos a través de correos electrónicos u otros medios.
- Ingrese a la página de Internet de la Fiduciaria digitando directamente la dirección www.fiduoccidente.com.co en el navegador. No ingrese a través de enlaces que haya recibido en correos electrónicos.
- Cambie su contraseña con frecuencia. Es una buena idea usar números, letras en mayúscula y minúscula combinadas. No construya su contraseña a partir de palabras como su nombre o apellido, ni tampoco de números como su fecha de nacimiento, documento de identidad, dirección o teléfono.
- Realice sus consultas y transacciones por Internet desde el computador personal de su casa u oficina. En algunos sitios públicos pueden estar instalados programas para capturar su información y suplantarlo.
- Instale y mantenga actualizado un software antivirus en su computador. Es recomendable tener también un software de protección de acceso (firewall personal).
- Mantenga actualizado el navegador de Internet de su computador.
- Antes de ingresar su usuario y contraseña verifique que está conectado a una página segura: la dirección de la página debe iniciar con el prefijo https y en la parte inferior derecha debe aparecer un candado cerrado.
- Cuando haya finalizado su consulta o transacción asegúrese de cerrar adecuadamente la sesión.
- Cualquier irregularidad o consulta, comuníquese a nuestra línea de atención al cliente a nivel nacional 018000521144, en Bogotá 2973060
- Para un óptimo funcionamiento de la Zona Transaccional de la Fiduciaria de Occidente, se recomienda tener en cuenta los siguientes aspectos técnicos:

  • Browser ó Navegador Internet Explorer 5.0 o superior.
  • Memoria RAM de 64 kb o superior.
  • Disponibilidad en disco duro de 300 MB o superior.
  • Procesador de 166 Mhz o superior.
  • Windows 98 o superior.
  • Configuración de Monitor de 800 x 600 pixeles.
  • Proveedor de acceso a internet rápido o módem que asegure una conexión a 33.000 bps o más.

Riesgos de Seguridad en Internet

A continuación encontrará una breve descripción de los riesgos de seguridad en Internet, como identificarlos y como evitar ser afectados.

PHISHING:

Intento de adquirir en forma fraudulenta información confidencial, como las contraseñas u otra información bancaria. El delincuente se hace pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica, por lo común un correo electrónico, indicando al cliente que ingrese a la página web oficial mediante un enlace adjunto en el correo, pero realmente el enlace se dirige a una página web fraudulenta con igual presentación, o muy similar a la oficial. Al ingresar a la página ficticia con el usuario y contraseña de la página oficial, esta información es capturada por el delincuente y es usada posteriormente para suplantar al cliente y hacer transacciones en su nombre.

Para evitar ser víctima del phishing, recuerde:

• Ingresar a la página de Internet de la Fiduciaria de Occidente digitando directamente la dirección www.fiduoccidente.com.co en el navegador. No ingrese a través de enlaces que haya recibido en correos electrónicos.
• Su usuario y contraseña de acceso a Internet son confidenciales. La Fiduciaria de Occidente nunca le solicitará estos datos a través de correos electrónicos u otros medios.
• Ante la recepción de correos electrónicos sospechosos con temas relacionados con Fiduciaria de Occidente, comuníquese a nuestra línea de atención al cliente a nivel nacional 018000521144, en Bogotá 2973060.

SPAM y CADENAS DE INTERNET

Se conoce como spam el envío de cualquier correo electrónico, masivo o no, a personas a través de este medio los cuales no han sido solicitados por el(los) destinatario(s), y que en algunas ocasiones se propagan a través del uso de cadenas de correo. Con ello se busca recolectar direcciones de correo electrónico reales para obtener beneficios económicos, transmisión de virus, captura de claves mediante engaño (phisihing), entre otros.

HOAXES

Mensajes de correo electrónico con contenido falso o engañoso, por lo general alarmante. Son ejemplos los mensajes sobre virus incurables, cadenas con campañas de solidaridad para enfermos incurables, quiebras bancarias, etc. que al parecer verdaderas y por su carácter alarmante tienden a ser distribuidas rápidamente, permitiendo así la recolección de cuentas de correo electrónico reales para usos no autorizados. Otra de sus principales características es no tener fechas específicas, lo que les permite tener vigencia en el tiempo.

¿Cómo evitar el spam y los hoaxes?

• No exponga en sitios públicos su dirección electrónica ni la de sus contactos
• Haga caso omiso a este tipo de mensajes y elimínelos inmediatamente de su buzón. No los reenvíe.

CÓDIGO MALICIOSO

Software que es intencionalmente introducido en un sistema con un fin malicioso o no autorizado. Son ejemplos de éste los troyanos, el spyware, rootkits, backdoors, keyloggers, etc.

Para reducir el riesgo de códigos maliciosos que pueden afectar a su PC y su información confidencial tenga presente:

- Instalar oportunamente las actualizaciones de seguridad del sistema operativo de su PC.
- Tener instalado y actualizado un sistema de antivirus.
- Instalar y configura un firewall.