

Guatemala, junio de 2011

Apreciable Cliente:

Con la finalidad de proteger su información personal, le sugerimos tomar en cuenta los siguientes consejos:

- Actúe con prudencia ante compañías o personas que desconozca y en las que no confíe.
- No responda a correos electrónicos que soliciten información de índole personal, si previamente no ha confirmado la legitimidad del remitente.
- No revele información que pueda ser considerada confidencial, incluyendo su clave de seguridad, su número de tarjeta de crédito, o cualquier otra información sensible, si previamente no ha confirmado la legitimidad de la consulta de información.
- Antes de introducir cualquier dato confidencial en una página web, verifique que en la parte inferior derecha de la página aparezca un icono representando un candado. Esto le garantizará que está navegando en un entorno seguro.
- Tenga cuidado al aceptar invitaciones a redes sociales donde desconocidos puedan obtener información de índole personal.
- Abra sólo aquellos correos electrónicos cuyo remitente conozca, en especial aquellos que tengan archivos adjuntos o que incluyan un enlace dentro del mismo. Esta es una forma muy sencilla de que su ordenador se vea afectado por un virus.
- Compruebe que su ordenador dispone de un programa antivirus actualizado. Estos sistemas antivirus necesitan de actualizaciones frecuentes para que sean efectivos en la protección de su ordenador contra nuevos tipos de virus que puedan surgir.
- Compruebe siempre la dirección de las páginas web a las que acceda, lo que en el lenguaje propio de Internet se conoce como URL. (Uniform Resource Locator).
- Asegúrese de que la URL que le interesa aparece en la casilla de la dirección situada en la parte superior de la ventana de su navegador. Algunas páginas web parecen legítimas cuando en realidad son fraudulentas.
- Recuerde cerrar su sesión cuando finalice todas sus tareas. En caso de estar utilizando un ordenador con personas a su alrededor, nunca deje la pantalla abierta.
- Utilice las claves de seguridad adecuadas para sus cuentas en Internet. Elija claves difíciles de adivinar por terceras personas, combine números y letras minúsculas y mayúsculas.
- Cambie su clave de seguridad con cierta regularidad. Se sugiere hacerlo por lo menos, una vez al mes. Evite la instalación de software de dudosa legitimidad.
- Si cuenta con accesos electrónicos a estados de cuenta debe mantenerse regularmente informado de los mismos y de las últimas operaciones realizadas. Estar informado es una excelente medida de control.

Grupo Financiero de Occidente se interesa por su seguridad.