INFORMACION IMPORTANTE

- Si recibe una llamada ofreciéndole premios, ofertas o promociones a nombre de Bantrab y le solicitan datos confidenciales como número de cuenta, saldo, clave de acceso o PIN, para entregarle el premio, evítelo y consulte la validez de dicha promoción en cualquiera de las agencias de Bantrab, o en Línea Directa llamando a nuestro Call Center 1755 o 2410-2600 o bien escribiéndonos directamente desde nuestra página http://www.bantrab.com.gt/.
- Antes de proporcionar información personal verifique la autenticidad de la persona que se la solicita.
- Si va a desechar su documentación financiera (estado de cuenta o voucher), previo asegúrese de destruirla.
- Asegúrese de recoger la correspondencia que recibe en su domicilio ya que puede ser utilizada por terceros con fines ilícitos.
- En caso de que alguno de nuestros Cajeros Automáticos Bantrab retuviera su tarjeta, debe reportarlo de inmediato. Recuerda hacer caso omiso de cualquier mensaje donde se te pida digitar tu PIN o cualquier otro número. No aceptes ayuda de extraños.

RECOMENDACIONES DE SEGURIDAD
PARA EL MANEJO DE CONTRASEÑAS

La clave de usuario y sus correspondientes contraseñas son, en muchos casos, el único medio para identificar a los usuarios de Banca por Internet, por lo que la administración de estos elementos se vuelve crítica debido a que si alguien los obtiene, puede asumir su identidad en el sistema y quedar facultado para realizar, en su nombre, todas las operaciones sobre sus cuentas registradas en su servicio de Banca por Internet, por lo que es importante tomar en cuenta lo siguiente:

- Memorice sus claves de acceso, no las escribas en ninguna parte, ni comparta con nadie.
- Procure que su clave de acceso sea una combinación de letras y números poco comunes y que no estén relacionadas directamente con su persona, nombres de familiares o mascotas, fechas de cumpleaños o cualquier contraseña que sea sencilla.
- Procure que su contraseña para accesar a su cuenta de Bantrab EnLínea no sea igual al que utiliza para accesar a otros sistemas, como correo electrónico o cuentas de otros bancos.
- Evite almacenar información financiera (usuarios, contraseñas, estados de cuenta, PINs, etc.) en su computadora personal.
- Cuando digite su contraseña de ingreso, procure que no le estén observando, no permita que nadie conozca su contraseña.
- Modifique su contraseña de ingreso, periódicamente, se recomienda que realice el cambio cada 30 días, o cuando considere que ésta pudo haber sido comprometida, asignado una contraseña totalmente nueva en cada ocasión y recordando combinar letras y números.
- No usar valores triviales, obvios o de fácil deducción por terceros.
- Utilizar por lo menos o más de ocho caracteres alfanuméricos.
- Si en algún lugar le requieren definir una “pregunta secreta” o pista para recuperar su contraseña en caso de olvido, procure que ésta no contenga la

contraseña en sí y evite utilizar respuestas obvias o que puedan ser conocidas por terceras personas. De preferencia evite utilizar esta opción si le es posible.

- Realice sus movimientos Bancarios en una computadora personal, evite computadoras de uso público que no sean de su confianza por ejemplo, de cafés internet, etc. En caso de tener que hacer uso de este tipo de computadoras, se le recomienda que cambie su contraseña, en cuanto antes, desde una computadora segura.

RECOMENDACIONES DE SEGURIDAD PARA EL MANEJO DE CONTRASEÑAS

BANTRAB

Uso del Equipo de cómputo utilizado para realizar transacciones financieras. Existen riesgos en el uso de los equipos de cómputo debido a que existen programas y dispositivos electrónicos que pueden sustraer o interceptar la información que se transmite y procesa, sin que el usuario lo pueda conocer y a su vez ser recuperada por terceras personas. Para disminuir estos riesgos, es importante tomar en cuenta lo siguiente:

- Realiza sus movimientos Bancarios en una computadora personal, evite computadoras de uso público que no sean de tu confianza por ejemplo, de cafés internet, etc. En caso de tener que hacer uso de este tipo de computadoras, se le recomienda que cambie su contraseña, en cuanto antes, desde una computadora segura.

- Evite, en la medida de lo posible, acceder al servicio de banca por Internet mediante hipervínculos. Digite la dirección de la página Web de la institución financiera directamente en su navegador. En algunas ocasiones los hipervínculos redirigen a otro tipo de páginas apócrifas que pretenden hacerse pasar por instituciones financieras para dar mal uso a la información ingresada.

- Nunca envíe información confidencial por medio de correos electrónicos, tales como: números de cuentas, tarjeta de crédito o débito, usuarios, contraseñas, etc.

- Al revisar su correo electrónico NO abra correos electrónicos sospechosos o de remitentes desconocidos, elimínelos y por ningún motivo descargue los archivos adjuntos. Tampoco conteste ese tipo de correos.

- Nunca ejecute directamente (doble clic) archivos adjuntos, guárdelos primero en una carpeta temporal (o en el escritorio) y revise luego esa carpeta con el antivirus actualizado, antes de tomar la opción de ejecutarlos (.EXE) o abrirlos (.DOC, .RTF, entre otros.).

- No haga clic en vínculos que aparezcan en ventanas de mensajes emergentes. Debido a que las ventanas de mensajes emergentes son frecuentemente producto del spyware, si se hace clic sobre alguna de ellas, se podría instalar software spyware en su equipo.

- Para cerrar las ventanas de mensajes emergentes se debe hacer clic en el icono "X" en la barra de título o presionar las teclas ALT + F4 en lugar de hacer clic en un vínculo "Cerrar" dentro de la ventana que es un engaño.

- No se aleje de su computadora cuando esté realizando un movimiento en eBantrab. Si desea alejarse cierra su sesión y verifique que su sesión ha terminado exitosamente.

- Desactive las opciones de recordar contraseñas y auto completar en su navegador.

- Verifique constantemente que sus movimientos por internet coincidan con sus voucher del cajero automático o sus voucher al utilizar su tarjeta en comercios.

- Si sospecha que su clave ha sido robada o que te ha llegado información sospechosa referente a transacciones electrónicas en Bantrab EnLínea, repórtelo de inmediato al número de servicio al cliente 1755 ext. 45000.

- Con el fin de mantener su computadora segura, actualícela con herramientas que le permitan detectar la ejecución de programas “maliciosos” tales como: spyware, virus, adware, entre otros, y que controlen las conexiones de entrada y salida (firewalls personales). Algunos de estos programas son proporcionados por el proveedor de su sistema operativo.

- Utilice una dirección de correo pública (gratuita) para suscribirse a todos aquellos productos, concursos, o para dar a conocer en grupos de interés y de noticias. De esta manera mantendrá privada su dirección primaria de correo electrónico (la de la empresa por ejemplo).

- No participe en cadenas de correo por más noble que la causa aparente ser, de esa forma obtienen las direcciones de muchas personas para enviar posteriormente las ofertas.

- El mejor método para evitar ser parte de las cadenas es nunca reenviarlas o responderlas. Para los temerosos o supersticiosos, infinidad de personas han roto las cadenas y no les ha sucedido nada. También han respondido unas cuántas y no se han vuelto millonarios, algunos de los niños que alegan enfermedad ni siquiera existen.