Existen varias formas en las que se puede robar su información personal de manera electrónica. Siga estos consejos para protegerse en Internet: **Protección de contraseñas**

- Nunca comparta su contraseña o PIN con nadie
- Nunca escriba su contraseña en un lugar que pueda ser fácilmente encontrada por los demás.
- Cuando cree su contraseña, no utilice información que pueda relacionarse fácilmente con usted (por ejemplo su fecha de nacimiento, número de seguro social o nombres de mascotas o pasatiempos).
- Use contraseñas que contengan tanto números como letras, preferentemente que no sean palabras reconocibles (ejemplo:7djskDer)
- La Federal Trade Commission (FTC) (Comisión Federal de Comercio) ofrece consejos útiles para contraseñas en http://www.onguardonline.gov/stopthinkclick.html.
- Utilice una contraseña única para cada sistema. Utilice siempre una contraseña distinta para cada sistema al que ingrese.
- Cambie con frecuencia las contraseñas de su cuenta en línea. Le recomendamos que cambie su contraseña cada 30 días.

Seguridad en línea

- Si suministra información financiera o efectúa un pedido por Internet, asegúrese de que el sitio sea seguro. Busque un URL que comience con "https://" y que tenga el "candado cerrado" () en la esquina inferior derecha de su navegador.
- Haga negocios solo con instituciones financieras y comerciantes de Internet que conozca y en los cuales confíe.
- Tenga cuidado con los sitios que intentan parecerse a una institución financiera. Tenga la precaución de revisar que la dirección web de su banco sea correcta.
- No responda a ningún correo electrónico o mensaje en una ventana emergente que le solicite la actualización o suministro de su información personal.
- Nunca deje su computadora sin vigilar mientras está usando cualquier servicio de inversión o de banca electrónica.
- Tenga la precaución de cerrar siempre la sesión y el navegador cuando haya finalizado una sesión segura.
- Sólo acceda a su información financiera personal en una computadora en la que usted "confíe". Los puestos de Internet y los cyber cafés no son tan seguros como su computadora personal.
- Instale, use y actualice regularmente programas anti–virus y anti–spyware en su computadora.
- Asegúrese de que su computadora esté actualizada con los parches de seguridad para su sistema operativo y aplicaciones. Los usuarios de Windows deben habilitar la función de actualización automática. Puede encontrar los parches de seguridad en el sitio web del proveedor. Consulte estos sitios periódicamente ya que estos parches se actualizan con frecuencia.
- Considere la posibilidad de usar un firewall personal para evitar que los hackers invadan

su computadora personal, especialmente si utiliza una conexión a Internet DSL o cable módem. Un firewall puede hacerlo prácticamente "invisible" en Internet y le ayudará a bloquear las comunicaciones de fuentes no autorizadas.

- Si utiliza una conexión inalámbrica, tenga la precaución de encender todas las funciones de seguridad, como por ejemplo la encriptación WPA. Cambie la contraseña y el SSID predeterminados de su enrutador inalámbrico.

Correos electrónicos seguros

- Si una oferta enviada por medio de un correo electrónico o en un sitio web parece demasiado buena para ser verdad, probablemente no lo sea.
- El correo electrónico no es seguro. Nunca envíe por correo electrónico su información financiera personal, como ser sus números de cuenta o su número de seguro social.
- No abra correos electrónicos o adjuntos de remitentes que no conozca. Incluso cuando conozca la fuente, sea precavido. Los adjuntos pueden contener virus troyanos que ponen en peligro la seguridad de su computadora.
- Tenga cuidado con las estafas por correo electrónico. Nunca responda a correos electrónicos no solicitados ni haga clic en correos sospechosos que le solicitan que valide la información de su cuenta o que brinde información personal.
- Utilice programas de software que filtren los correos electrónicos "spam" e identifiquen los mensajes sospechosos.
- Deshabilite la función de "visualización previa" en su programa para correo electrónico. Esta función puede significar un riesgo a su seguridad.
- Use mensajería segura cuando esté disponible. Nuestra aplicación de banca electrónica cuenta con una función de mensajería segura a la que puede acceder una vez que haya iniciado sesión.