www.powersoft.net.ec

RECOMENDACIONES DE SEGURIDAD EN INTERNET

Sugerimos poner en práctica las siguientes recomendaciones de seguridad para el uso de Internet:

Sobre privacidad.

- Nunca divulgue sus nombres usuario y contraseñas. Sus nombres usuario y contraseña son únicos y sin ellos, nadie puede tener acceso a sus cuentas o servicios.
- Cambie periódicamente sus contraseñas, más aún si sospecha que alguien extraño conoce.
- Evite usar software u otras opciones, con la finalidad de que no tenga que escribir su contraseña la siguiente vez que tenga acceso al mismo sitio desde la misma computadora. Este tipo de software le podría dar a otros usuarios acceso a sus cuentas o servicios si llegaran a utilizar su computadora.
- No deje su computadora desatendida mientras tenga acceso a servicios bancarios en línea
- Siempre salga de los Servicios en Línea cuando haya terminado de realizar sus operaciones.
- Borre los archivos temporales de Internet siempre que salga de los Servicios en Línea. Cada vez que accede a Internet, su navegador guarda automáticamente una copia de las páginas de Internet que usted ha visitado.
- Nunca envíe información confidencial (tal como números de cuenta de cualquier tipo, usuario, contraseña, etc.) por medio de correo electrónico.
- Revise sus estados de cuenta en forma regular y reporte a su banco inmediatamente cualquier discrepancia.
- En caso de extraviar su tarjetas electrónicas, comuníquese inmediatamente con su banco.

Para proteger lo que guarda en su computadora

- Utilice un software de firewall. Antes de conectar su computadora a Internet, instale un firewall personal de marca reconocida o habilite el que trae Windows en caso de utilizar este sistema operativo. El firewall es un hardware o software que le ayuda a prevenir que intrusos o virus ingresen a su máquina.
- Actualice el sistema operativo y los programas de su computadora. Si está utilizando cualquiera de los programas de Windows utilice la opción Windows Update. Si utiliza Linux actualice mediante apt-get, yum o el gestor de paquetes instalado.
- Instale un antivirus. Instale y mantenga actualizado un antivirus de marca reconocida. El software antivirus es un programa que puede venir preinstalado en su computadora o que necesita instalar, para ayudarle a proteger su computadora contra virus, "Caballos de Troya" y otros intrusos no deseados.

- Deshabilite la compartición de archivos. La compartición o intercambio de archivos es una facilidad de Windows, que permite a otras computadoras tener acceso a su computadora personal, aún por medio de Internet. Para hacer esto, seleccione Inicio, posteriormente Configuración, Conexiones de red y acceso telefónico. Con el botón de la derecha, haga clic en Conexión de área local y posteriormente en Propiedades. En la pantalla que aparece, asegúrese que la casilla Compartir impresoras y archivos para redes Microsoft esté desactivada. Finalmente haga clic en Aceptar.

Sobre la suplantación de identidad en Internet (phishing)

- Si recibe un correo electrónico o una ventana de mensaje emergente solicitándole información personal o financiera, no responda, ni tampoco haga clic en el enlace o vínculo del mensaje.

- No envíe información sensible a través de Internet. Antes verifique si el sitio Web es seguro.

- Nunca responda a solicitudes de información personal a través de correo electrónico. Si tiene alguna duda, póngase en contacto con la empresa que supuestamente le ha enviado el mensaje.

- Ponga atención en el URL del sitio Web que visita. Los sitios Web maliciosos pueden parecer idénticos a los sitios legítimos, pero el URL puede tener variaciones o un nombre de dominio diferente.

- Asegúrese que el sitio Web utiliza cifrado (https//:....).

- Instale una barra antiphishing en su navegador, conocidas también como spam blocker. Estas herramientas están disponibles para los principales navegadores de Internet.

Basado en información publicada en:
http://www.scotiabankinverlat.com/Tips/TipsDeSeguridad.htm
http://www.seguridad.unam.mx/usuario