Recomendaciones de seguridad en Internet

Cuando utilice su conexión a Internet, sugerimos tener en cuenta las siguientes recomendaciones:

- Sobre privacidad:
  - Nunca divulgue su nombre de usuario ni contraseña. Su nombre usuario y contraseña son únicos y sin ellos, nadie puede tener acceso a sus cuentas o servicios.
  - Cambie frecuentemente su contraseña, más aún si sospecha que alguien extraño la conoce.
  - Evite usar programas 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 termine de utilizar 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 el sistema operativo que utilice. Firewall es un programa que le ayuda a su computadora a prevenir que intrusos o virus ingresen.
  - Actualice el sistema operativo y los programas de su computadora. Por ejemplo, si utiliza Windows active la opción de Actualizaciones automáticas que encontrará en el Panel de Control.
  - Instale un programa antivirus y manténgalo actualizado. Un antivirus es un programa que puede venir preinstalado en su computadora o que necesita instalar, para ayudarle a proteger su computadora contra virus y otros programas intrusos no deseados.
  - Deshabilite la compartición de archivos en su computadora. 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. Si utiliza Windows, 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 o “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 que el sitio Web sea 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 a la dirección del sitio Web que visita. Los sitios Web maliciosos pueden parecer idénticos a los sitios legítimos, pero la dirección puede tener variaciones o un nombre de dominio diferente.
    - Asegúrese que el sitio Web tiene una dirección que comienza con https://: esto significa que el sitio maneja encriptación en la transmisión de los datos.
    - Instale una barra antiphishing en su navegador. Estas herramientas están disponibles para los principales navegadores de Internet.

Fuente:
http://www.scotiabankinverlat.com/es-mx/Acerca-de-Scotiabank/seguridad.aspx
http://www.seguridad.unam.mx/usuario-casero/index.html