CONSEJOS DE SEGURIDAD EN INTERNET

Le sugerimos poner en práctica las siguientes recomendaciones de seguridad para el buen uso de Internet en su hogar u empresa:

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 las conoce. No utilizar claves estándares para el acceso a las cuentas de usuarios. Se recomienda usar un password que contenga al menos 3 referencias de los siguientes caracteres: números, letras mayúsculas, letras minúsculas, símbolos; además que tenga mínimo 8 caracteres de longitud.

- 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 sus tarjetas electrónicas, comuníquese inmediatamente con su banco.

- No reveles información importante sobre tu persona: En las redes sociales como Facebook, Google+ o Twitter, o en las salas de chat, fotologs o cualquier sitio donde un desconocido puede acceder a información personal de otras personas, evita dar detalles de la escuela o la facultad en la que estudias, del lugar donde trabajas y principalmente del lugar en el que vives. Evita también poner a disposición de extraños, datos o fotos que brinden cualquier detalle relevante sobre tu persona, por ejemplo, fotos en las que aparezca la fachada de su casa o la patente de tu automóvil. Nunca publiques tu número de teléfono a través de estos medios, tampoco informes el lugar en el que estará en las próximas horas, o el lugar que frecuentas. Si estos datos están dirigidos a tus amigos, envíalos de manera personal, pues toda y cualquier información relevante sobre ti, puede ser usada indebidamente por personas con malas intenciones.

- Cuidado al registrarte: Muchos sitios webs exigen que te registres para usar algunos de sus servicios, pero esto puede ser una trampa. Por ejemplo, si un sitio web pide tu número de tarjeta de crédito sin ser una página de ventas, las posibilidades de que se trate de un engaño o una estafa son grandes. Además, tu información personal puede ser entregada (vendida) a empresas que venden, por ejemplo, productos por teléfono. O peor aún, su e-mail puede ser agregado a listas de SPAMs.

  Por eso, antes de registrarte en un sitio web haz una búsqueda en internet para verificar si esta dirección está involucrada con alguna actividad ilegal. Evalúa también si es estrictamente necesario registrarse.

PARA PROTEGER LA INFORMACIÓN 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 XP SP2 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.

- 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.

- Si usas programas para descargar archivos, como Emule o Ares, o sueles descargar archivos de sitios webs de descargas, estate alerta a cada cosa que bajes. Al finalizar una descarga, verifica si el archivo no posee algo extraño, por ejemplo, más de una extensión (como "programa.mp3.exe"), tamaño muy pequeño o información de descripción sospechosa, pues muchos virus y plagas pasan por archivos de audio o vídeo para engañar al usuario. Además de esto, siempre examina el archivo que descargaste con un antivirus.

- También ten cuidado de aquellas webs que te soliciten la instalación de un programa para continuar la navegación, o para acceder a algún servicio. Desconfía también de las ofertas de programas milagrosos, capaces de doblar la velocidad de tu computadora o de mejorar la performance.

- Cuidado con los e-mails falsos: Tal vez hayas recibido en algún momento un e-mail que informa sobre una deuda con una empresa de telefonía, o que afirma que uno de

tus documentos no es legal. O un mensaje que te ofrece premios, o tarjetas virtuales de amor. Te intimaron a una audiencia judicial?

- Evita sitios webs de contenido dudoso: Muchos sitios webs contienen en sus páginas scripts capaces de buscar fallas del navegador de internet, principalmente Internet Explorer. Por eso, evita navegar en sitios webs pornográficos, de contenido hacker o que tengan cualquier contenido dudoso.

- Cuidado con los adjuntos en un e-mail: Este es uno de los problemas más comunes. El e-mail es una de las principales formas de diseminación de virus. Ten cuidado al recibir mensajes que te piden abrir un archivo adjunto, principalmente si el e-mail proviene de alguien que no conoces. Para aumentar tu seguridad, puedes chequear el archivo adjunto con un antivirus, inclusive si esperabas recibir ese archivo.

- Cuidado al realizar compras en internet o al usar sitios webs de bancos: Hacer compras a través de internet es una gran comodidad, pero sólo hazlo en aquellos sitios de vendedores reconocidos. Si estás interesado en un producto que se ofrece en un sitio web desconocido, haz una búsqueda en internet para descubrir si alguien tuvo problemas con esa empresa.

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 scam blocker. Estas herramientas están disponibles para los principales navegadores de Internet.