Para ***HablaSip*** tu Seguridad es la más importante, te recomiendo leas detenidamente estos consejos.

Consejos para mejorar su seguridad en Internet

Antivirus y cortafuegos son programas imprescindibles para mantener nuestro ordenador a salvo de las amenazas informáticas, pero no basta con instalarlos. Si quiere estar bien seguro debe adoptar algunas precauciones.

1. El mejor software de seguridad no sirve de nada si no se actualiza regularmente: configure la actualización automática y controle periódicamente el estado del programa. También hay que actualizar el sistema operativo.

2. **Configure bien el cortafuegos y antivirus**. Los sistemas operativos más populares (Windows XP yVista, Mac OSX y Linux) cuentan con un cortafuegos: hay que desactivarlo antes de instalar uno nuevo, pues dos programas de este tipo activos al mismo tiempo en el mismo ordenador pueden provocar un conflicto entre sí. Si decide instalar por separado cortafuegos y antivirus, empiece por el antivirus.

3. **Los productos de Microsoft** son el principal blanco de los piratas informáticos. Limitará los riesgos si elige software de otras marcas. Puede optar por ejemplo por un navegador alternativo a Internet Explorer.

4. **Antes de abrir ficheros o imágenes** que vengan de algún soporte externo o que le hayan enviado por correo electrónico, ponga en marcha el antimalware.

5. **Nunca hay que responder los correos sospechosos**, ni abrir los archivos que lleven adjuntos, ni hacer clic sobre los links que aparezcan en el mensaje. No envíe datos personales: si manda un mismo correo a distintos destinatarios, use la copia oculta, para no mostrar a todos las direcciones de los demás.

6. **Si debe dejar una dirección de correo en un foro**, por ejemplo, es mejor crear una dirección específica (incluso temporal) para este tipo de usos.

7. **No envíe por correo electrónico datos sensibles**. Si tiene que operar con la banca on line, es más seguro teclear directamente la dirección de la página a la que desea acceder en vez de usar un enlace que haya

recibido en un correo, por ejemplo. Cerciórese antes de que se trata de una conexión segura (lo puede comprobar porque empieza con https y tiene un candado en la parte baja del navegador).

8. Extreme las precauciones cuando use un ordenador público.

9. **Recuerde realizar periódicamente copias de seguridad** de todos los archivos en un soporte externo: así no perderá todo el material si las precauciones no han bastado para evitar el ataque informático.

10. **Si sólo dispone de antivirus y cortafuegos**, sepa que algunos navegadores y clientes de correo electrónico incorporan protección antispam y programas antiphishing, según el caso. Utilícelos. Y recuerde que sólo debe descargarse programas de sitios seguros.

Privacidad:

La elección y uso de un conjunto usuario: contraseña, es fundamental en el ámbito de la seguridad informática y en la protección de la privacidad, una contraseña mal escogida o sin una buena protección puede ser fácilmente vulnerada y provocar serios problemas de seguridad tanto a nivel personal como corporativo. Por esta razón es fundamental que el cliente tome todos los correctivos necesarios para evitar ser víctima de ataques y/o fraudes electrónicos. El usuario es responsable de velar por la seguridad de las contraseñas asignadas, para el uso en los distintos servicios ofrecidos por Hablasip.

• Su nombre de usuario y contraseña son personales, ninguna otra persona debe tener acceso a ellos.

• No utilice contraseñas obvias o que se deriven de información personal o preferencias del usuario como el mismo nombre de usuario, el nombre de la mascota, nombres de personas, artistas preferidos, estilo de música, número de identificación, teléfono, fechas de nacimiento, etc.

• Cambie en forma periódica su contraseña, con una periodicidad de por lo menos 6 meses, si sospecha que su contraseña fue comprometida, cambiarla de forma inmediata.

• Tener una longitud de 6 o más caracteres, mientras más larga es la cadena, más complicado es vulnerar la seguridad de la clave.

• En los casos donde se soporte la contraseña debería ser una mezcla de caracteres alfabéticos (A..Z, a..z), numéricos (0..9) y especiales (!#$%&/...), en el caso de las letras se puede utilizar una mezcla de mayúsculas y minúsculas.

Suplantación de identidad (*Phishing*)

Phishing, con este término en ingles que significa pescar, se denomina a la práctica fraudulenta de suplantación de sitios web, principalmente de instituciones financieras, realizada por estafadores que envían mensajes de correo electrónico o mensajes de aparición automática en sitios web (popup ads) para atraer con engaños a los consumidores y sustraer su información personal o financiera
sin que se den cuenta. Para evitar que lo "pesquen" con este anzuelo:

• No responda a los mensajes electrónicos o de aparición automática (pop-up ads)
mediante los que le soliciten información personal o financiera ni haga clic sobre los vínculos o enlaces incluidos en estos mensajes.

• No utilice la función copiar y pegar (copy and paste) para colocar el enlace en el
navegador de internet — los "pescadores de información" o *phishers* pueden lograr que los vínculos aparenten llevarlo a un sitio Web pero en realidad lo conectan a uno diferente.
• Algunos estafadores envían un email que parece provenir de un negocio legítimo en el que le informan que su acceso a los sevicios en línea ha sido bloqueado y en el texto del mensaje le indican que acceda a un sitio web para actualizar sus datos y/o desbloquear su acceso.

• Un banco jamás le pedirá su número secreto por correo electrónico. Los números
secretos deben ser utilizados sólo en la página del servicio (Bancos, Servicio de Pagos, Tarjetas de crédito, etc.)

• Verifique que la dirección del sitio web inicie con la determinación del protocolo
https:// en lugar de **http://** que es el que se encuentra normalmente en las páginas web.

• No envíe información personal ni financiera por correo electrónico.

• Revise los estados de cuenta de su tarjeta de crédito y cuenta bancaria tan pronto como los reciba para verificar si se le han imputado cargos que usted no ha autorizado.

• Tenga cuidado al abrir archivos electrónicos adjuntados o al descargar archivos de mensajes electrónicos recibidos, independientemente de la identidad del remitente.

• Reenvíe estos mensajes de "phising" a la compañía, banco u organización cuyo nombre fue falsamente invocado como remitente del mensaje de correo electrónico.

• No deje desentendida su computadora mientras se encuentra en los sitios web de sus servicios financieros.

• Siempre utilice la opción **Salir** que se encuentra en el sitio de su banco, para cerrar la sesión en línea, no basta con cerrar la ventana o pestaña del sitio, acostúmbrese a eliminar la información temporal de estos sitios en su navegador.

• En caso de extraviar sus tarjetas de acceso a sus servicios financieros en línea, comuníquese de inmediato con su institución financiera para realizar el bloqueo de la misma.

• Si usted fue afectado por este tipo de ataque, puede acceder a los servicios de la Fiscalía General de la Nación o Defensoría del Pueblo.

Protección Infantil

En la actualidad el uso de las tecnologías de la información por parte de los niños se realiza desde edades más tempranas, internet se ha convertido en una herramienta sumamente importante para el aprendizaje de los niños, pero también se debe tener en cuenta que la libertad que existe en el medio la hace sumamente peligrosa.

Es deber de los padres el control de uso de las tecnologías de la información y el acceso a los servicios de internet, se recomienda la supervisión de los padres o apoderados de los niños o adolescentes en la administración del uso que le den a esta herramienta.

Los adultos deben involucrarse proactivamente en las actividades de sus hijos en internet y controlar el contenido, existen varias alternativas desde gratuitas hasta de pago, que permiten el control de contenido, el usuario deberá verificar cual es la que mejor se adecua a sus preferencias.