JEAPC. COMUNICACIONES

PROVEEDOR DE INTERNET

LE RECOMIENDA SEGUIR LOS SIGUIENTES TIPS DE SEGURIDAD PARA EL USO SEGURO DE LOS SERVICIOS DE INTERNET Y TRASMISION DE DATOS

Privacidad:

La elección de uso de un conjunto de 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 ataque y/o fraudes electrónicos. El usuario es responsable de velar por la seguridad de las contraseñas asignadas, para el uso en los distintos servidores ofrecidos por Jaime Pesantez.

- Su nombre de usuario y contraseña son personales, ninguna otra debe tener acceso a ellos
- No utilice contraseña obvias o que se deriven de información personal o preferidas del usuarios como el mismo nombre de usuario, el nombre de la mascota, nombres de personas, artistas preferidos, estilo de música, número de identificación, teléfonos, fecha de nacimiento, etc.
- Cambie en forma periódica su contraseña, con una de por lo menos 6 meses, si sospecha que su contraseña fue comprometida, cambiarla de forma inmediata.
- Tener una longitud de 6 o más característica, mientras más larga es la cadena, más complicado es vulnerar la seguridad de la clave.
- En los caso donde se soporte la contraseña debería ser una mezcla de característica alfabéticos (A...Z, a...z), numéricos (0....9) y especiales (¡#$%&/.....), en caso de las letras se puede utilizar una mezcla de mayúscula y minúsculas.

Suplantaciones de identidad (*phishing)*

Phishing, con este término en ingles que significa pescar, se denomina a la práctica fraudulenta de suplantaciones de sitios web, principalmente de instituciones financieras, realizadas por estafadores que envían mensajes de correo electrónicos o mensajes de apariciones automática en sitios web (pop-up ads) para atraer con engaño a los consumidores y sustraen 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 funciones copiar y pegar (copy and paste) para colocar el enlace en el navegador de internet – los “pescadores de información” o *phishers* pueden lograr que vincule aparentes llevarlos a un sitio Web pero en realidad lo conectan a unos diferente.
- Algunos estafadores envían un email que parecen prevenir de un negocio legítimo en el que le informan que su acceso a los servicios en líneas 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 pedirán su número secreto por correo electrónico. Los números secretos deben ser utilizados solo en páginas del servició (Bancos, Servicios de pagos, Tarjetas de créditos, etc.).
- Verifique que la dirección del sitio web inicie con la determinación del protocolo **https:**// en lugar de **http:**// que se encuentran normalmente en las páginas web.
- No envié 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 mensajes electrónicos recibidos, independientemente de la identidad del remitente.
- Reenvíe estos mensajes de "phising" a la compañía, banco u organizaciones cuyo nombre fue falsamente invocado como remitente del mensaje de correo electrónico.
- No deje desatendida su computadora mientras se encuentre en los sitios web de sus servicios financieros.
- Siempre utilice la opción **salir** que se encuentre en el sitio de su banco, para cerrar la sección en línea, no basta con cerrar la ventana o pestaña del sitio, acostúmbrese a eliminar la información temporal de este sitio en su navegador.
- En caso de extraviarse sus tarjetas de acceso a su institución financieros en líneas, comuníquese de inmediato con sus instituciones financieras para realizar el bloqueo de la misma.
- Si usted fue afectado con este tipoi de ataque puede acceder a los servicios de la Fiscalía General de la Nación o defensoría del pueblo.

- Tener los programas -antivirus, firewal, etc etc- de proteccion como al igual algun HW de respaldo para poder protegerte -como los router o algunos switch que actuan como ruter y firewall-.1. No reveles información personal por Internet. Establece restricciones a tu información personal en sitios de redes sociales.
  - Llena con cuidado formularios de registro. Cerciórate de que estás llenando ligas de empresas conocidas y confiables.
  - Evita sitios que muestren violencia y/o pornografía, pueden ser de alto riesgo
  - . No te conectes a sitios de descarga de música gratuita. Además de infringir leyes de autor, esto puede dañar tu computadora
  - Actualiza de forma periódica tu sistema operativo
  - Cambia claves y contraseñas con frecuencia.
  - Respalda tu información y utiliza contraseñas robustas.
  - Al descargar programas desconocidos, revisa que tengan licencias. Bajar software accidentalmente puede instalar en su computadora virus informáticos.
  - No compartas información personal de tus contactos con otras personas en Internet, atenta contra tu seguridad y la de ellos.
  - No concretes citas con "amigos" virtuales, generalmente son desconocidos
  -

Protección Infantil

En la actualidad el uso de la tecnología de la información por parte de los niños se realiza desde edades más tempranas, internet se ha convertido en una herramienta sumamente muy importante para el aprendizaje de los niños, pero también se debe tener en cuenta que la libertad que existe en medio se hace sumamente peligrosa, es deber de los padres el control de uso de la tecnología 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 dan a estas herramientas, los adultos deben involucrarse en proactivamente en las actividades de sus hijos en internet y controlar el contenido, existen varias alternativas desde gratuitas hasta el pago, que permiten el control de contenido, el usuario deberá verificar cual es la mejor se adecua a sus preferencias.