Informáticas I

2. Protección de información y Hardware

Debemos tomar medidas cuando usar computadoras no sólo para mantener nuestros archivos e identidad fuerte y segura, sino también nuestros equipos. Tanto como un coche, tomando las medidas pertinentes para proteger un equipo asegurará funcionará conforme a su diseño y no nos falles.

2.1 Protegiendo el equipo

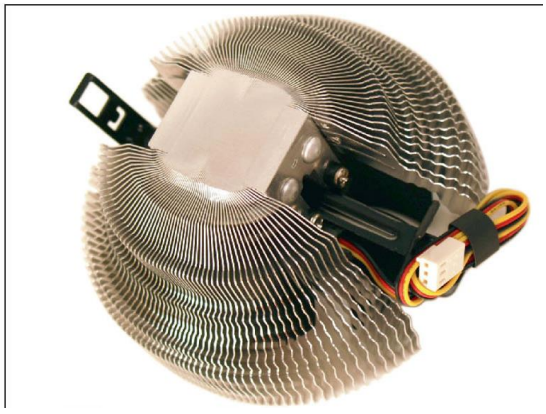
Si el procesador y otros componentes de un sistema de sobrecalientan, el sistema obtendrá inestable y componentes comenzará a fallar y se dañan. Partes de computadora dañada son caras y es esencial tanto para los usuarios privados y corporaciones para refrigerar sus máquinas.

El calor máximo de un ordenador debe ser 185 grados.

Un sistema adecuadamente refrigerado debe mantener una temperatura de 90 – 110 grados.

Dispositivos para enfriar un sistema incluyen:

- Ventiladores de la CPU y la caja – ventiladores extraen el aire caliente de la caja para evitar el sobrecalentamiento.
- Enfriadores – se sientan encima del procesador. Contiene ventilador y disipador de calor. El disipador de calor extrae calor del procesador y el ventilador disipe el calor.



- Herramientas para la prevención de polvo – como las que se discuten en la lección 2

La tarjeta de video atrae las energías más y algunas tarjetas de vídeo pueden adquirirse con un ventilador conectable a enfriar el sistema.

Al proteger el ordenador, la protección más básica comienza con la lucha contra sobretensiones y picos.

Protectores de voltaje son dispositivos económicos que filtran la energía eléctrica para eliminar sobretensiones y picos de tensión antes de que lleguen a su equipo. Protectores contra sobretensiones son muy baratos, a partir de alrededor de $10 para un protector de corriente 4 salidas.

Al comprar a un protector de voltaje, menor el dejar-por voltaje, mejor su equipo estará protegido. También es aconsejable comprar un protector contra sobretensiones que tiene una garantía que cubre no sólo el dispositivo de protección contra sobretensiones, pero el equipo que está protegiendo.

2.2 Protegiendo tus archivos

Fallo del sistema, virus, corrupción de archivos o algunos otros problemas pueden causar pérdida de datos.

Como ya comentamos en la lección 2 uno de los mejores métodos de protección de sus datos es por los respalda.

Nunca confianza datos importantes a sólo media y eso es por qué siempre debemos tener múltiples copias y almacenarlos en dispositivos diferentes.

Nunca te fíes de los datos importantes en un solo dispositivo y es por eso que siempre debemos tener varias copias y almacenarlos en diferentes dispositivos.

Después de la copia de seguridad, debe eliminar un archivo y tratar de recuperarlo para asegurar que el proceso de copia de seguridad ha funcionado bien.

Para proteger sus archivos, software antivirus es una de las mejores líneas de defensa.

Antivirus - es un software de computadora utilizado para prevenir, detectar y eliminar virus informáticos malintencionados.

Software antivirus puede protegerte de:

- Virus, Spyware, Malware
- Protección de Firewall
- Compras en línea y transacciones bancarias segura
- Protección de la privacidad
- Evita el espionaje
- Robo de datos
- Fraudes de phishing

Software antivirus también nos permite buscar sitios web y ser alertados antes de acceder a un sitio peligroso por la exploración de sitios web en los resultados de búsqueda y basado en información previa conocida acerca de un sitio Web.

2.3 Protegiendo su identidad

Aparte de proteger tus archivos es crucial que protegerse. Tu identidad en línea es muy vulnerable y debe tomar pasos que su información personal no es robado.

Maneras de proteger su identidad

- Utiliza un firewall, software antivirus y software anti-spyware.
- Crear contraseñas fuertes
- Mantenga actualizado el sistema operativo, y navegador.

Crear contraseñas que mezclar 10 o más letras, números y caracteres especiales. No usar la misma contraseña para más de una cuenta.

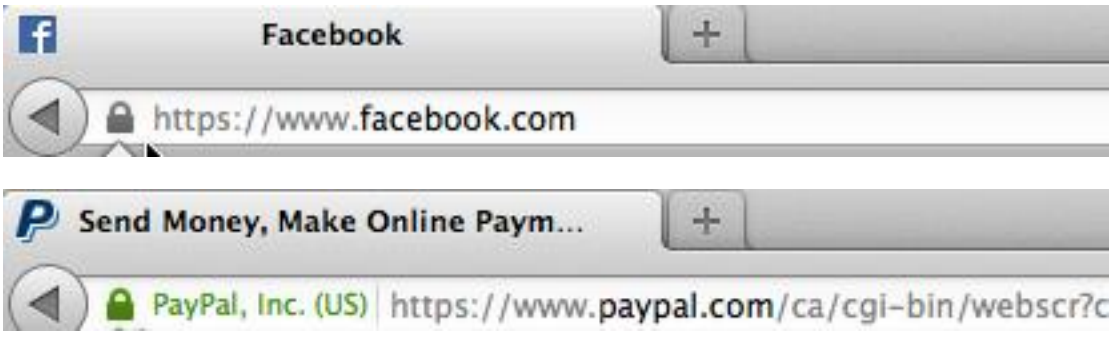
Utilice el software antivirus, software anti-spyware y un firewall en tu computadora. Protección contra intrusiones e infecciones que pueden comprometer su computadora o contraseñas mediante la instalación de parches de seguridad para su sistema operativo y otros programas.

Un Consejo es configurar el sistema operativo, navegador y sistema de seguridad para actualizar automáticamente de su computadora.

Cuando envías sensible información sobre la Internet sólo lo hacen si hay un icono de "candado" en la barra de estado de su navegador. Esto significa que su información estará a salvo cuando se transmite. Si la barra tiene una cerradura y es de color verde que significa que se utiliza un cifrado más fuerte y el sitio web es incluso más seguro que de costumbre.

Si un sitio web no pasa información sensible que no habrá ningún bloqueo pero está bien utilizar el sitio Web. Un ejemplo popular de tal un sitio web es youtube.com

Ciertos aspectos del sitio web pueden ser seguros, por ejemplo un socio de YouTube mirando sus ingresos por publicidad estaría mirando a través de una página cifrada como puede contener información de impuestos, seguridad social y hasta números de cuentas bancarias.



No confiar siempre en Wi-Fi gratuita

Antes de utilizar una red pública de Wi-Fi, ver si su información estará protegida. Si usted usa un sitio web de cifrado, protege solamente la información que usted envía a y desde ese sitio. Si usas una red inalámbrica segura, toda la información que usted envía en esa red está protegida.

Los ladrones de identidad dependen de gente haciendo compras y conectando a las cuentas bancarias a través de estas redes Wi-Fi no seguras para ellos para robar números de tarjetas de crédito y otra información importante.

Estas redes no seguras son el resultado de ser creada por una persona que no sea como experto en el sector de seguridad. Corresponde a los consumidores a ser siempre conscientes y conocedores.

Muchas compañías grandes han sido atacadas vía Wi-Fi no garantizado con los años y ha resultado en cientos de miles de cuentas comprometidas.