Guía 20 minutos para la Seguridad Informática de su PC

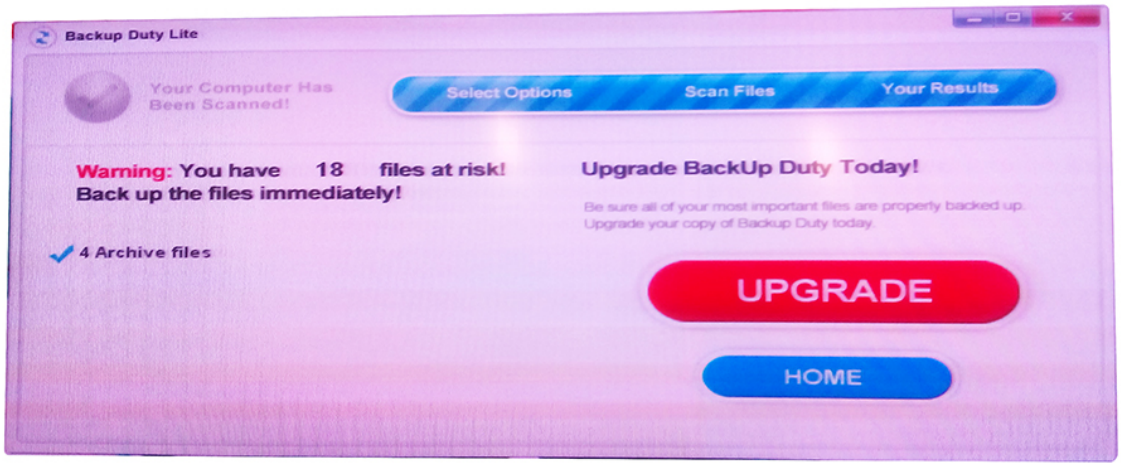
Con la gran cantidad de Malware y las técnicas cambiantes utilizadas por los hackers y spammers, es casi seguro que su equipo se enfrenta a varias amenazas de seguridad todos los días. En este artículo hemos introducido 20 de los pasos más rápidos y más esenciales para la seguridad de su PC o equipo informático en general.

Gastar veinte minutos en la prevención puede ahorrar más de 20 horas intentando arreglar el daño. Si usted toma la tarea de dedicar unos minutos para configurar y mejorar la seguridad de su equipo, reducirá drásticamente las probabilidades de que esas amenazas tengan éxito y perjudiquen su PC.

En esta guía de consejos sobre la seguridad de los datos digitales, vamos a darle una serie de consejos para el cuidado de su Pc.

Va a encontrar diversos consejos y tips sobre :
la protección de sus datos, la correcta instalación de las medidas de seguridad de su sistema, el adecuado uso del correo electrónico, problemas inalámbricos, contraseñas seguras ... ¡y mucho más!

Con más de 140.000 virus informáticos (conocidos a día de hoy) y 85 millones envíos de Spam cada día, aumenta considerablemente la probabilidad de que su ordenador entre en contacto con programas maliciosos, malware cómo virus, gusanos y software.



Una vez que su ordenador es infectado, **tareas simples como navegar por la web puede ser muy frustrante** ya que la velocidad del equipo se reduce drásticamente, siempre y cuándo en el mejor de los casos aún pueda conectarse a Internet.

Dado que el malware hoy por hoy campa a sus anchas por los vastos recovecos digitales, la única solución real es prevenir que infecten su equipo por completo.

¿Pero cómo?

En esta "Guía de 20 Consejos" vamos a enseñarte 20 pasos de seguridad a tener en cuenta si navegas por Internet para reducir las probabilidades de que se infecte su ordenador mientras navega por la red.

Mediante la implementación de estos 20 pasos, simples y directos, podrá disminuir la probabilidad de infección por malware.

Como dice el refrán :
"Antes de poder correr, debe aprender a caminar"

FUNDAMENTOS para DETECTAR Y ELIMINAR LAS AMENAZAS

El primer paso hacia la seguridad informática, es instalar un software básico y necesario para detectar y eliminar futuras amenazas.

Utilice un firewall

Un servidor de seguridad es una especie de muralla alrededor de su ordenador que identifica y filtra las amenazas mientras que deja pasar la información segura a su ordenador.

Un servidor de seguridad sirve para realizar un filtrado entre su ordenador e Internet, el uso de un buen servidor de seguridad es el primer paso en el camino hacia la seguridad informática.

Sugerencias : Si tu sistema operativo es Windows, ya tiene un firewall instalado. Así que la única cosa que hay que comprobar es si lo tienes activado.

Para habilitar el servidor de seguridad, vaya al Panel de control y seleccione "Conexiones de red". A partir de ahí, haga clic en el derecho de su conexión a Internet activa, y seleccione el menú "Propiedades". Por último seleccione la pestaña "Avanzado" y marque la casilla "Firewall de conexión a Internet".

Si usted no tiene Windows o simplemente quieres actualizar más allá de la protección estándar que ofrece Windows. Hay una serie de opciones de firewall de software de terceros en el mercado, entre los que destaca Norton Personal Firewall.

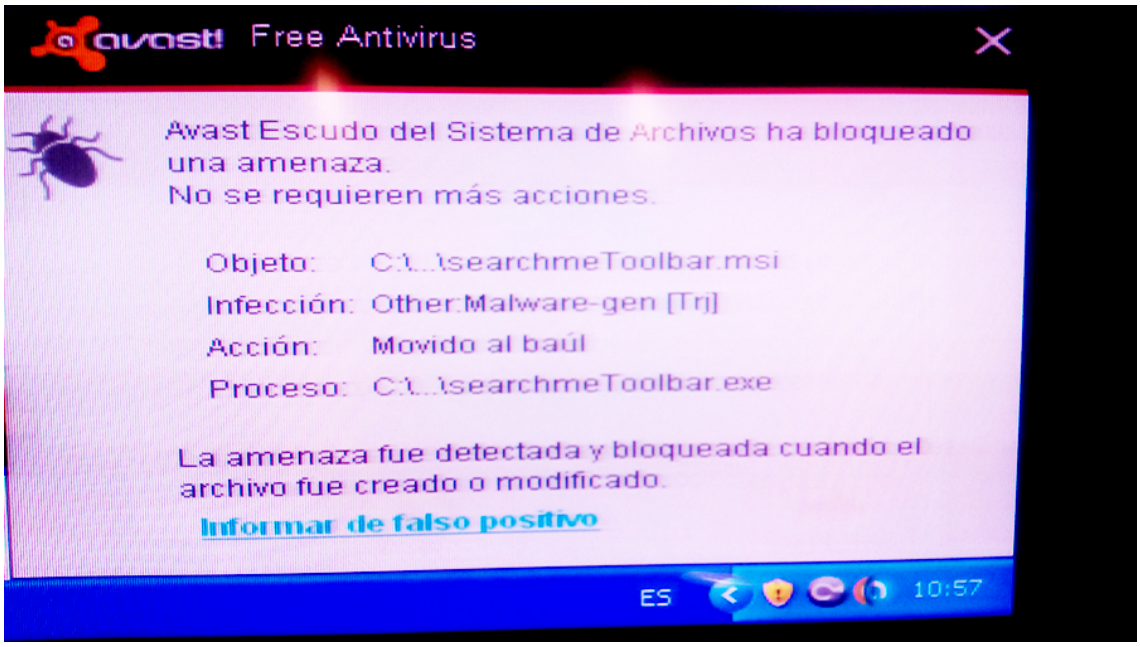
Para aquellos que quieren ahorrar algo de dinero, una buena opción gratuita de firewall es PC Tools Firewall Plus 1.0

Instalar y actualizar software antivirus

Un buen firewall filtrar muchas de las amenazas que atacan a su ordenador, sin embargo algunos tipos de malware siempre van a encontrar el camino de colarse en su PC. Por ejemplo, los virus, gusanos, troyanos y otras formas de malware pueden encontrar la forma de instalarse en su equipo por diversos medios que un firewall no puede detectar como la descarga de archivos adjuntos desde su correo electrónico maliciosos o en la descarga de archivos desde Internet, que pueden presentarse cómo inofensivos y finalmente convertirse en maliciosos infestando su ordenador.

Así qué para proteger su PC , necesita actualizar su ordenador regularmente con un software antivirus solvente. Recuerde que solo debe de tener instalado un solo software para tal gestión, ya que cuándo un ordenador dispone de más de uno, no son efectivos.

De forma que mientras un servidor de seguridad (bien instalado y adecuado) protege su equipo desde el exterior, un programa antivirus trabaja desde el interior de su equipo a la caza de virus ocultos para poder eliminarlos al tiempo que escanea archivos adjuntos o descargas, antes de que puedan infectar su ordenador.



Sugerencias : Para aquellos de ustedes que no les importa gastar algo de dinero en seguridad **Avast** ofrece uno de los mejores productos en el mercado antivirus personal. Si quieres probarlo antes de comprarlo, ofrecen una **versión gratuita** de su software antivirus.

En el caso de los gratuitos, sirven para que pueda limpiar su ordenador y volver a empezar de nuevo, en casos puntuales probablemente en breve esté de vuelta en el mismo punto de partida con su equipo infectado o casi inutilizable.

Instale y ejecute el software anti-spyware

Para que los firewalls y programas antivirus estén activos en su ordenador, hay que instalar también un software anti-spyware. Con el adecuado programa anti-spyware le

proporcionar a su equipo, un aumento significativo de la seguridad.

Un estudio reciente estima que 9 de cada 10 ordenadores conectados a Internet están actualmente infectadas con algún tipo de spyware. Hoy en día, la forma más común de malware que los usuarios se encuentran en Internet, es spyware. El spyware puede tomar una variedad de formas, sin embargo, algunos de los efectos más comunes son la aparición de ventanas emergentes no solicitadas; robo de información personal; supervisión de su actividad por Internet, para su comercialización; peticiones a otros sitios web de envío de publicidad no deseada (conocido como Spam).

Sugerencias : El programa más popular para la eliminación de spyware es de Anti-Malware Bytes que viene con una variedad de paquetes que incluye la edición Professional, y la edición Personal gratis. La ejecución de un programa anti-spyware puede tender a retrasar su ordenador, por este motivo ejecute el software cuando no tenga que utilizar su equipo.

Instalaciones adicionales

Además de los programas de software de seguridad universales necesarios mencionados anteriormente, hay un par de instalaciones software que pueden ser de primera necesidad para usted, dependiendo del uso que le dé a su ordenador.

Sugerencias : Si usted navega habitualmente por sitios de juegos y apuestas, o sitios pornográficos. Todos ellos son especialmente vulnerables a un tipo de malware llamado rootkits . Si este es su caso, es absolutamente esencial que instale el software anti-rootkit como Malware bytes Anti-Malware para garantizar la integridad de su PC, e incluso aunque su perfil no pertenezca a una de esas vulnerables categorías, es una excelente opción tenerlo activado.

Una buena opción para ayudarle a identificar y eliminar rootkits desde su PC, es Sysinternals o Windows Sysinternals. Se trata de una colección de programas para Windows para usuarios con conocimientos avanzados, profesionales o administradores de sistemas. Ocupa poquísimo espacio en el disco, y ofrece funciones que por defecto Windows no incluye o mantiene ocultas e inaccesibles. Entre sus programas, encontrarás soluciones para gestionar discos y archivos, personalizad la configuración de Windows sobre redes, mantener bajo control los procesos del sistema y obtener información al detalle de cualquier elemento de Windows que pasa desapercibido a otros programas similares.

Control parental : La instalación de software de control parental no se trata sólo de determinar a qué sitios tiene acceso su hijo. Es un paso importante para mantener su ordenador libre de malware. A menudo los niños o mayores pasan mucho tiempo navegando en sitios de juegos, o realizan descargas de software gratuito. Desafortunadamente todas estas actividades son muy peligrosas en lo que a infecciones de malware se refiere. Uno de los controles de los padres es ZoneAlarm Internet Security Suite que además incluye varios tipos de servidores de seguridad así como la protección de virus y spyware.

AFINANDO CONFIGURACIÓN Y REALIZACIÓN DE AJUSTES DE USO

Ahora que ya ha instalado el software de seguridad para PC, hay una serie de puntos débiles específicos en la armadura de su equipo que necesitan ser apuntalado haciendo algunos ajustes personales, de comportamiento, para compensar la debilidad de seguridad en particular o mejoras para minimizar su vulnerabilidad.

Reforzar la seguridad de su navegador web

Todos navegamos por Internet a través de un navegador web. Y si utiliza Chrome, Firefox, Internet Explorer, Opera o cualquier otro, son un punto débil en las defensas de cualquier ordenador. Los hackers a menudo dirigen sus ataques contra el ordenador al centrarse en los defectos en los navegadores o sus plugins y el uso de las descargas para acceder a su dispositivo descargando malware adjunto, a lo que realmente quiso descargar desde el navegador sin que lo sepa.

Debido a esta amenaza, las actualizaciones de seguridad del navegador web son un primer paso importante en su reacondicionamiento de seguridad de su PC.

Sugerencias: La actualización de seguridad más fácil a llevar a cabo es simplemente cambiar el explorador o navegador que tiene por defecto para acceder a Internet.

Internet Explorer (también denominado Explorer) de Microsoft se somete al mayor número de amenazas de seguridad, por lo que el cambio a una alternativa popular más segura, como Mozilla, Firefox, Opera, y Google Chrome mejorarán drásticamente la seguridad de su PC de forma inmediata.

Para aquellos empeñados en el uso de Internet Explorer, debería elevar el nivel de seguridad de la configuración por defecto a "modo alta" y especificar qué sitios web son de confianza suficiente para evitar el filtro de seguridad del navegador. Puede hacer esto mediante la apertura de una nueva ventana del navegador, seleccionando el menú "Herramientas", seguido de "Opciones de Internet". A partir de ahí elegir la pestaña "Seguridad" y, finalmente, arrastre la barra hasta el nivel "Alto".

Instale los últimos Service Pack del Sistema Operativo

Los hackers están constantemente desarrollando nuevos tipos de malware, algunos de los cuales tratan de explotar las debilidades de un sistema operativo para entrar en el equipo. Por lo tanto, en función de la versión de Sistema Operativo que utilice es importante instalar siempre los últimos "Service Pack de Windows (SP)" con el fin de mantener su equipo seguro. Microsoft publica parches y actualizaciones para sus sistemas operativos Windows al menos una vez al mes.

Sugerencias : Descargar parches sólo directamente desde el sitio oficial de Windows y nunca de cualquier otro lugar. Los spammers a menudo crean hábilmente parches infectados falsos y los publican en sitios web propios o ajenos con el fin de engañar a la gente e infectar sus computadoras mediante la descarga e instalación de los mismos. De este modo, mediante la descarga de los parches exclusivamente desde el sitio oficial de Windows, que es fuente fiable, puede minimizar las posibilidades de que alguna vez encuentre un parche falso en el primer lugar de la búsqueda que pueda hacer por Internet.

Seleccione software seguro y actualícelo regularmente

Probablemente haya visto alguna vez divertidos anuncios publicitarios entre Mac y PC en la televisión, donde se habla sobre el gran número de virus y exploits a los que está expuesto un PC que corra con Windows en relación a los Mac (iMac, MacBook) de Apple.

Por desgracia, es cierto que el sistema operativo y el software que usted seleccione juega un papel importante en el número de amenazas a los que se enfrenta el equipo. Aunque el número de amenazas que afectan a Mac crece paulatinamente día a día, al menos por ahora, los virus en su mayoría se concentran en programas de Microsoft. En consecuencia, si está ejecutando un sistema operativo de Windows, u otra aplicación de Microsoft, es extremadamente importante que actualice con frecuencia su aplicación con todos los nuevos parches que Microsoft pone a disposición. En pocas palabras, si una aplicación tiene actualización, la probabilidad de que su equipo tenga una amenaza de seguridad será mayor. Así que para evitar las brechas innecesarias en la seguridad, mantenga siempre su software importante actualizado hasta la fecha.

Sugerencias : Ejecute las actualizaciones automáticas de Windows cuando están disponibles. Ello minimiza el riesgo de agujeros y vulnerabilidades del Sistema Operativo.

Si aún no ha adquirido un equipo, infórmese sobre las diferencias en los niveles de amenazas que tienen los diferentes sistemas operativos y aplicaciones (básicamente entre Windows y Mac). Si bien es probable que no tenga sentido que usted seleccione un sistema operativo en función de las amenazas intrínsecas que pueda tener aparejadas, sí podría tener sentido a la hora de elegir un programa alternativo ofrecido por un competidor de similares características, pero que tuviese menos riesgos de seguridad.

Desactivar el intercambio de archivos en sus discos duros

Mientras la seguridad de su router WiFi le ayuda a mantener a raya a los hackers impidiendo el acceso a la red, ¿qué pasa con el potencial daño de las personas que ya tienen acceso legítimo a la red? Tener un cortafuegos sin duda ayudará, pero puede no ser suficiente. Una de las mejores maneras de limitar su exposición a los daños dentro de su propia red es mediante la prohibición de acceso a archivos para compartir en las máquinas. Esto es especialmente importante si usted está en un gran red o utiliza una red wifi abierta, como en una biblioteca de la universidad o en un edificio de oficinas, en las que no se sabe quién podría estar potencialmente navegando a través de su PC.

Sugerencias : Utilice el plugin AllPeers en el navegador web Firefox para permitir el intercambio seguro en internet.

Utilice el "uso compartido seguro" a través de uno de los clientes VoIP (Skype) o VoIM (Google Talk , Yahoo Messenger , Windows Live Messenger) como una opción alternativa.

Tenga cuidado al descargar

Aunque no todo programa gratuito es malo, el viejo dicho de que en la vida nada gratis vale la pena, es cierto en general cuando se trata sobre las descargas de Internet. Los spammers a menudo esconden malware peligroso en los programas de ordenador que se ofrecen de forma gratuita a modo de descarga en Internet. Cuando usted descargue estos programas gratuitos, sin saber que están infectados, es fácil que puedan eludir el firewall y el antivirus de protección, y a menudo como consecuencia provocan graves infecciones de malware.

Sugerencias : Si es posible, busque un sitio Web de confianza, como ZDNet o VNUnet, desde la que realizar la descarga de los archivos deseados.

Si descarga a través de programas tipo eMule o Torrent, asegúrese de escanear los archivos que reciba en busca de virus y otros programas maliciosos, ya que muchos servidores de archivos no comprueban la integridad de los documentos que acogen.

ENVÍO POR CORREO ELECTRÓNICO DE FORMA SEGURA

El correo electrónico fue diseñado originalmente para permitir a académicos y científicos comunicarse entre sí. Fue creado con la idea de que sólo las personas de confianza enviarían archivos de ida y vuelta, las debilidades en la seguridad del correo electrónico nunca fueron una preocupación mientras que la tecnología se estaba desarrollando. Por desgracia, los spammers y hackers llegaron junto con la popularidad del correo electrónico, pero para entonces la tecnología ya era demasiado popular como para rediseñarla. Como resultado de las debilidades inherentes de seguridad, es muy importante tomar las medidas necesarias para fortalecer la seguridad de su correo electrónico a través de extensiones, complementos y protecciones, adaptando el modo de utilizar su correo electrónico.

Utilice un cliente de correo electrónico de primer nivel

Sólo porque todos los clientes de correo electrónico entregan su correo electrónico, no significa que son igualmente eficaces cuando se trata de la seguridad del PC. Un cliente de correo electrónico eficaz debe proporcionar a su equipo con otra capa de protección al filtrar con eficacia todos los mensajes de correo electrónico no deseados con destino a su bandeja de entrada, así como proporcionar algún escaneo de virus básico en los ficheros adjunto del correo electrónico.

Sugerencias : Google Mail (Gmail) es uno de los mejores clientes de correo electrónico basados en la web, que le proporciona la parte superior de la línea de filtrado de spam que mantendrá su bandeja de entrada libre de casi todos los mensajes no deseados. Sin embargo, desafortunadamente su capacidad de análisis de virus deja mucho que desear, por lo que debería analizar manualmente todos los archivos adjuntos de su correo electrónico personal mediante el escáner de virus antes de descargarlos.

Thunderbird de Mozilla es un muy respetado, premiado, y combate muy bien el spam de su correo electrónico. Una vez tenga la configuración de Thunderbird hecha, usted estar· bien seguro de tener su bandeja de entrada libre de spam.

Maneje los adjuntos del correo electrónico con cuidado

Al descargar un archivo adjunto, el ordenador supone que usted sabe lo que está haciendo. En consecuencia, su firewall no comprobará el accesorio para asegurarse de que es seguro, lo que deja sólo una exploración superficial por su cliente de correo electrónico como la única protección entre un archivo adjunto y el ordenador. Dado el bajo nivel de seguridad de los archivos adjuntos, no es ninguna sorpresa que los hackers a menudo traten de ocultar sus programas dañinos en estos archivos adjuntos haciendo spam a su dirección de email. De hecho, se estima que el 90 por ciento de los virus entrar en los ordenadores de esta manera. Dadas estas estadísticas, es importante seguir siempre las mejores prácticas al manejar todos los archivos adjuntos de correo electrónico en su bandeja de entrada.

Sugerencias : No abra archivos adjuntos de desconocidos, o incluso de empresas de renombre, no importa lo oficial o conoce el correo electrónico parece ser. Los spammers a menudo utilizan técnicas muy creativas para hacer que sus mensajes de correo electrónico y sus archivos adjuntos parezcan legítimos, y se están haciendo cada vez más sofisticados en eso. Así que simplemente examinar de cerca los correos electrónicos con archivos adjuntos antes de la descarga ya no es una estrategia de seguridad suficientes. En su lugar, debe adoptar una estricta política de seguridad analizando al remitente del mensaje y yendo a la página web de la compañía directamente para obtener la información necesaria en su lugar.

Si la computadora de un amigo está infectado, es posible que usted reciba correo electrónico con archivos adjuntos infectados con virus que parecen ser (o mejor diríamos que en realidad es) de ellos. Por lo tanto, un remitente conocido por sí solo no es suficiente para garantizar que un archivo adjunto es seguro. Si usted no está esperando un archivo adjunto, llamada, mensajería instantánea o VIP de esa persona, comprueba de alguna manera que tenían la intención de enviarlo antes de abrir el archivo adjunto.

No haga clic en enlaces de correo electrónico al azar

Un técnica común de phising o estafa es la de insertar un enlace en un mensaje de correo electrónico de aspecto auténtico, pero en realidad ser totalmente falso que conduce a un sitio web malicioso. Estos mensajes de correo electrónico por lo general tratan de engañar a la gente para que haga clic en el enlace y renunciar a la información personal con el fin de supuestamente "confirmar su información financiera", o incluso sólo para "darse de baja" de un boletín de noticias que nunca se inscribieron en el primer lugar. Así que recuerde: los enlaces incorporados en correos electrónicos puede plantear un riesgo enorme seguridad del PC.

Sugerencias : No haga clic en enlaces en correos electrónicos cuestionables. Empresas de renombre pueden enviar un correo electrónico diciendo que hay un problema con su cuenta, pero nunca van a incluir un enlace "para su conveniencia" que proclama haber perdido todos sus datos.

Incluso si usted personalmente sigue correo electrónico las mejores prácticas, los miembros de la familia que utilizan cuentas de correo electrónico compartidas pueden aún sin saberlo hacer clic en enlaces maliciosos e infectar su computadora. En consecuencia, es posible que desee desactivar la opción de ver los correo electrónico en formato HTML" para que los enlaces incorporados en correos electrónicos ya no funcionen, y así como prevenir a los miembros de la familia en algunas de las técnicas más comúnmente utilizadas por los estafadores y hackers.

Establecer filtros de correo electrónico

Proveedores de Servicios de Internet (ISP) de buena reputación están desarrollando continuamente actividades de filtrado de spam efectiva con el fin de reducir al mínimo la cantidad de spam que llega a su cliente de correo electrónico. Y del mismo modo que el nivel adicional de filtrado ayuda a reducir los niveles de spam que llegan a su bandeja de entrada, por lo que también se puede añadir su propio nivel de filtrado suplementario mediante la creación de sus propios filtros de correo electrónico personal. Mientras que el filtro y el filtro ISP cliente de correo electrónico trabajen juntos, limitarán drásticamente la cantidad de spam que recibe, y además sólo mediante la adición de un componente de filtrado manual en el filtrado personalizado podría llegar a estar cerca de los niveles de spam cero.

Sugerencias : Comience con un cliente de correo electrónico eficaz y añada filtros personalizados. GMail permite crear una serie de alias de correo electrónico a su dirección de correo electrónico, lo que le permitir· dividir mensajes del email entrantes en carpetas que dependan de la variante particular del correo electrónico o al que fue enviado. Así, cada vez que usted se inscribe en un nuevo boletín, puede utilizar una nueva variante en el correo electrónico. Si un boletín termina vendiendo su nombre a los spammers, simplemente puede bloquear ese correo electrónico y listo, quedando detenido el flujo de correo no deseado e identificado que la newsletter están vendiendo en secreto la electrónico de contacto de los lectores al mejor postor.

Si usted no tiene acceso a los alias de correo electrónico, puede lograr exactamente lo mismo mediante la creación de múltiples cuentas de correo electrónico gratuito y designar uno específicamente para suscripciones a boletines informativos. Si no quiere estar al día con todas las cuentas de correo electrónico o puede incluso utilizar una cuenta de correo electrónico o con electrónico como 10minutemail que le permitirá confirmar su suscripción a un boletín o servicio, pero que no va a poner su verdadero correo electrónico en peligro de recoger spam.

LA PROTECCIÓN DE CONTRASEÑA

Usted nunca pondría en peligro a su familia con una clave en la alarma tan simple como: "1 ... 2 ... 3". Pero a pesar de ello muchas personas se exponen a ser hackeados cuando seleccionan contraseñas que son demasiado simples o que se cambian con muy poca frecuencia.

Mantenga ocupados a los Hackers

Hackers utilizan una variedad de técnicas para tratar de adivinar las contraseñas. Uno de los métodos más eficaces simplemente es ejecutar un programa informático que intenta aleatoriamente palabras comunes y combinaciones de números. Sabiendo esto, usted debe adaptar su contraseña para que no pueda ser fácil de adivinar por "Hackers Diccionario".

Sugerencias : Utilice contraseñas seguras de al menos 8 caracteres de longitud, con una mezcla letras mayúsculas y minúsculas y cifras de números. Ejemplo: AxV37TtP0.

Nunca utilice palabras o nombres comunes en su contraseña. De hecho, lo que no parecen palabras es una forma efectiva de mantener ocupados a los hackers para que no adivinen su contraseña.

Cambie sus contraseñas con regularidad.

No importa lo segura que pueda parecerle su contraseña, con el tiempo llegar· a ser comprometida. Sin embargo, al modificar su contraseña con regularidad, puede estar seguro de que en el momento en que un hacker se apoderase de su contraseña usted ya la habría cambiado.

Usar una variedad de diferentes contraseñas

Es la naturaleza humana para que la gente se siente cómoda con un nombre de usuario y contraseña en particular, y para mantener el uso de una y otra. Debido a que los hackers lo saben, a menudo se dirigen a sitios menos garantizados con el fin de recoger los nombres de usuario y contraseñas, sabiendo que esas mismas combinaciones usuario y clave serán probablemente las mismas que se utilizan en los sitios más garantizados (y más valiosos), tales como los bancos en línea.

Sugerencias:

Utilice diferentes contraseñas y nombres de usuario para todas las aplicaciones basadas en la Web. Si está abrumado por la idea de tener que recordar una docena de contraseñas diferentes, adquiera a un sistema para organizar numéricamente contraseñas de modo que incluso si se olvida una contraseña podrás adivinar rápidamente más tarde mediante la comparación con las contraseñas que recuerde.

Sea creativo con sus nombres de usuario. Casi todo el mundo utiliza una combinación de la primera inicial / apellido, por lo que un hacker puede simplemente suponer que en cualquier base de datos hay un JPerez, un JSmith1, y así sucesivamente. Asegúrese de que su nombre de usuario no es algo que se pueda adivinar fácilmente.

La contraseña protege el acceso al equipo

Mientras que muchas personas están dispuestas a establecer contraseñas complejas para los servicios en línea, a menudo se resisten a hacerlo para proteger el acceso físico a su equipo. Sin embargo la verdad es que casi todos los ordenadores está en peligro de ser visitados por personas que no tienen autorización para hacerlo. Empezando por sus propios hijos, o quien limpia su oficina mientras usted está en el trabajo, con frecuencia la persona que accede a su equipo no tiene la intención de hacer daño a usted o a su computadora pero accidentalmente puede comprometer la seguridad del mismo, y ello es fácilmente subsanable con una contraseña para acceder al equipo físico.

Sugerencias : No sólo añadir una contraseña a su perfil personal, sino también para todas las cuentas de invitados. Una vez más, usted no está solo preocupado con que alguien maliciosamente intente dañar su equipo, a menudo el mayor peligro proviene de los usuarios de Internet sin experiencia que son simplemente curiosos.

Utilice un protector de pantalla con protección de contraseña. Tan bien es bueno proteger con contraseña sus inicios de sesión, porque si usted es como la mayoría de la gente, a menudo dejar· el equipo inactivo en lugar de apagarlo inmediatamente después de que haya terminado de usarlo. Así podrá eliminar esta vulnerabilidad mediante la creación de un protector de pantalla protegido con contraseña para volverlo a poner en marcha si el equipo se queda inactivo por más de unos pocos minutos.

Considere la posibilidad de crear un acceso directo del escritorio para bloquear su equipo informático si usted es el tipo de persona que olvida asegurar las cosas. Es simple y conveniente hacerlo.

WIRELESS PROTECTION

Con el reciente aumento de las redes inalámbricas y puntos de acceso en todo el mundo, el foco de los ataques de Internet ha cambiado una vez más a un nuevo punto débil en la seguridad de un PC, las conexiones wifi. Afortunadamente, en tan sólo unos pocos pasos, usted puede mantener su equipo a salvo de intrusos inalámbricos.

Proteja su red inalámbrica

Si usted tiene una red inalámbrica, es importante protegerse de hackers y chupones de conexión, así como de otros usuarios no deseados, de su red wifi. Hay varias opciones que puede establecer para hacer que su red inalámbrica y PC sean más seguros.

Sugerencias : Cifrado de su red wifi: la configuración predeterminada para cifrar su red es con WEP, un estándar de cifrado tan corto y vulnerable con tanta facilidad, que a menudo es considerado como poco mejor a que no tengan el cifrado en absoluto. En su lugar, actualizar su red inalámbrica a la mucho más fuerte norma de protección WPA2.

Muchos hackers simplemente se pasean alrededor de los vecindarios en busca de redes wifi tituladas "default" o "Linksys" con el fin de identificar a aquellos que no ha tomado aún medidas básicas para proteger su red inalámbrica. Evite esta obviedad a los hackers tomando un minuto para cambiar el nombre de su red Wi-Fi.

Simplemente ocultando su emisión SSID y la aplicación de filtrado de direcciones MAC puede limitar drásticamente el acceso externo a la red pues los hackers no sabrán que su red wifi existe. Recuerde que un hacker casi siempre toma el camino de la menor resistencia, por lo que al detener su difusión SSID impedir a los hackers seguir adelante y buscar otro sitio para víctimas más

No utilizar la conexión wifi del vecino

Aparentemente conexiones wifi sin protección en lugares convenientes tales como complejos de apartamentos y aeropuertos pueden tener encerrona. Mientras que estas conexiones no seguras pueden simplemente ser de un individuo que no ha tomado el tiempo para proteger su red, también podrían ser "honeypots", o trampas puestas por los hackers para enganchar sus datos personales.

Sugerencias : Si es absolutamente necesario usar WiFi "público", asegúrese de cifrar y proteger los datos que su ordenador envía. También debe cifrar sus mensajes instantáneos si usted planea usar el servicio desde un punto de acceso vulnerable.

Nunca firme en las cuentas financieras (bancarias, PayPal, etc.) mientras está conectado a una red pública. De hecho, trate de escribir tan poca información privada como sea posible cuando se accede a Internet a través de cualquier conexión wifi que no esté garantizada.

Si tienes un Smartphone con un plan de datos inalámbricos, es posible que pueda crear su propio punto de acceso wifi en lugar de tener que conectarse a una red pública no segura.

PROTECCIÓN FISICA

No importa cuántos pasos usted toma para cifrar, proteger con contraseña, o cualquier otra manera electrónica para proteger el equipo; ninguna de esas medidas significar nada si alguien roba físicamente su computadora portátil. En consecuencia, una parte importante de cualquier reforma seguridad de la PC es tomar medidas que minimicen el riesgo y la exposición de robo físico.

Disfrazar su portátil

Mire a su alrededor: es probable que hayas visto personas que llevan bolsas en las que se nota claramente que transportan sus portátiles. Aunque no hay ninguna regla que diga que usted no pueda, llevar bolsos alternativos reducen la posibilidad de que alguien va a tratar de apoderarse de su ordenador portátil en un aeropuerto o en cualquier otro lugar. De la misma manera que se oculta su monedero o el iPod antes de salir de su coche, disfrazando su ordenador portátil reduce el conjunto de los posibles ladrones, y por tanto las posibilidades de que su ordenador sea robado físicamente.

Sugerencias : Asegúrese de que la bolsa alternativa es resistente al agua y acolchada.

Una alternativa conveniente a la funda del ordenador portátil es una bolsa de mensajero, pero también se podría tratar de una bolsa de deporte, o si te sientes realmente friki, incluso una caja de pizza . Si la falta de atractivo estético no le molesta, su nueva bolsa podría lucir un aspecto degradado y sucio (mientras por dentro esté limpia que es donde irá su portátil), esto educe aún más la probabilidad de robo. Boblbee ofrece una gran multiusos rígida mochila que mantener su computadora segura y sin señalizar lo que estás llevando. Uno de los modelos, concretamente el modelo Megalópolis está diseñado específicamente para contener y ocultar un ordenador portátil, así como protegerlo de la caída ocasional.

Utilice soluciones antirrobo

Todo el mundo utiliza su ordenador portátil en un lugar público como una biblioteca o librería cafetería. ¿ No le preocupa que se lo puedan robar si lo dejase desatendido por un segundo? Bueno, pues podría pasar. Afortunadamente, hay un par de pasos que puede tomar para minimizar el riesgo de que esto ocurra, y para mejorar las posibilidades de recuperación del ordenador si lo hace.

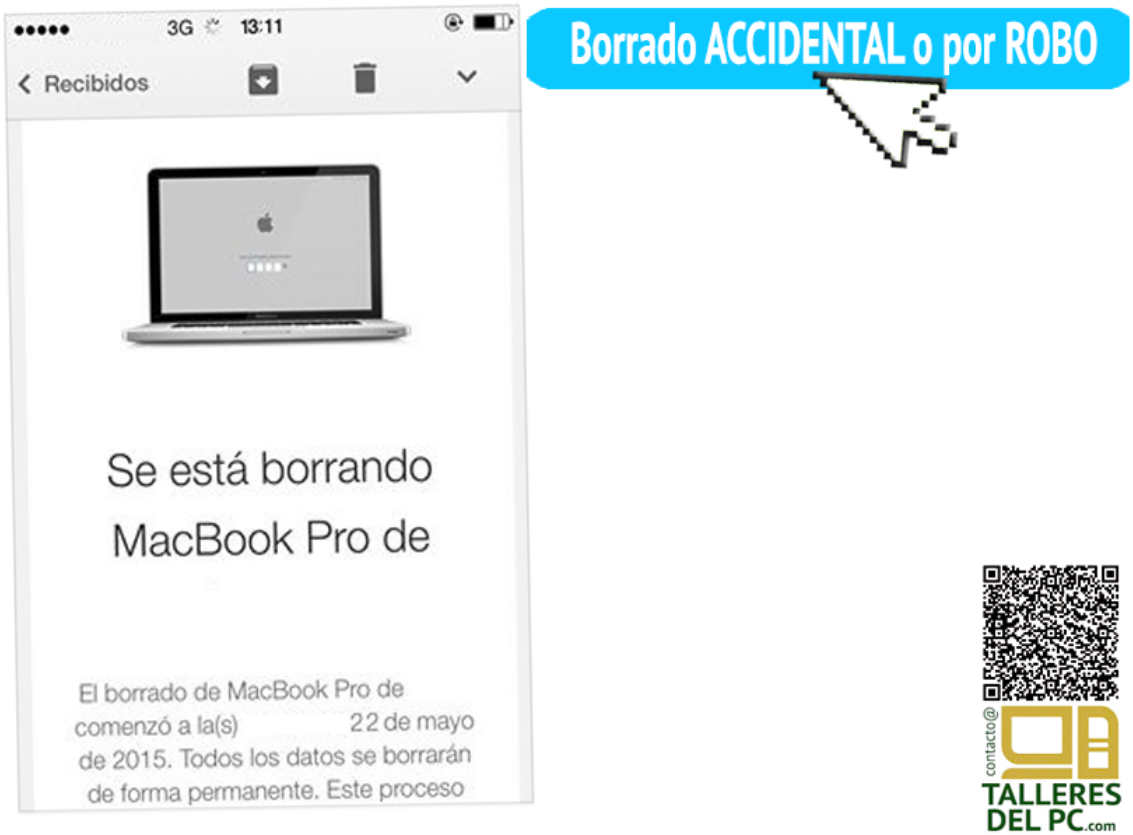
Sugerencias : Una técnica que sirve como un elemento de disuasión y una herramienta de recuperación es conseguir Placa de Seguridad de STOP, pegatina permanente en su computadora portátil para indicar que el dispositivo se puede rastrear por la policía en caso de robo.

Otra medida de seguridad creativa es la instalación de software de seguimiento de modo que en caso de robo, su equipo portátil en secreto transmitir su ubicación a un centro de control en cuanto el ladrón tenga acceso a Internet.

SEGURIDAD INFORMÁTICA

"La privacidad en Internet es posible, pero no está al alcance de los despreocupados" *Jeffrey Rosen, profesor de Derecho.*

La seguridad informática comprende tanto al software (base de datos, archivos, etc.) como al hardware. En ambos, ante un robo no tenemos nada que hacer, hoy en día los "amigos de lo ajeno" se han profesionalizado y pueden desconectar tu copia de seguridad, como es en el caso de esta imagen, en el nuestro cliente pudo ver a través de su IPhone como le borraban el contenido de su propio portátil recién sustraído,

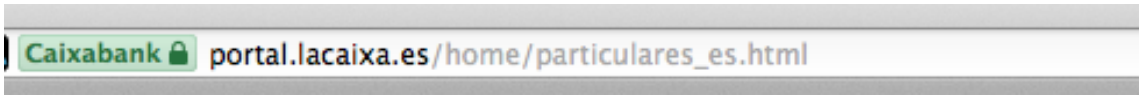


contacto@TALLERES DEL PC.com

o este caso real por el ataque de un virus a través del correo electrónico del usuario. Existen muchos tipos de amenaza en forma de "Virus Informático" que pueden infectar tu ordenador. Su puerta de entrada es a través del software.

Existe un riesgo ante la información que usted tenga en su ordenador. De forma, que no abra ninguna URL que desconozca, o correo electrónico recibido en su mail personal o laboral. Antes verifique, si tiene duda de su real procedencia.

A la hora de acceder a espacio como su banco online, asegúrese de que ese portal es fiable, entidades como un banca online o sistemas de pago como PayPal, dispones de un candado en la URL que confirma que es un portal web seguro.



Sugerencias : además de poner en marcha lo aquí indicado para la seguridad de tu ordenador.

- Visita la web del Instituto Nacional de Ciberseguridad (INCIBE). Organismo dependiente de Red.es y del Ministerio de Industria, Energía y Turismo de España. Tiene su sede oficial en León (España), y una oficina en Madrid.

- La oficina de Seguridad informática OSI para particulares

- El Instituto Nacional de Seguridad para empresas

- Y la entidad pública Red.es es que trabaja para que la sociedad española aproveche al máximo el potencial de Internet y las nuevas tecnologías.

ro portal midiscovirtual.es dónde podrás hacer a golpe de clic en unos minutos tu propia cuenta para disponer de una copia de seguridad de todos los datos de tu Pc o Mac.

Pues como reza nuestro lema

"Más vale prevenir que lamentar"

Invitech Online SL, desde 2007 estamos dedicados por completo a la tecnología desde diferentes soportes y marcas.

Después de encontrarnos con muchos siniestros en nuestro taller y tienda Talleres del PC, muchos de estos posibles de evitar.

Pusimos en marcha nuestro propio servicio online en la nube para realizar con toda comodidad, rapidez y a un precio más que razonable (lo que valen dos cafés al mes) el servicio de copia de seguridad para ordenadores PC y Mac.

Esperamos que su incursión por nuestros espacios sea de su interés. Si Ud. es empresa disponemos de varias tarifas pensadas para los profesionales y todo lo relacionado con el trabajo en Red.

Mi Disco Virtual .es

Cláusula de Confidencialidad y Protección de Datos

Powered by INVITECH online