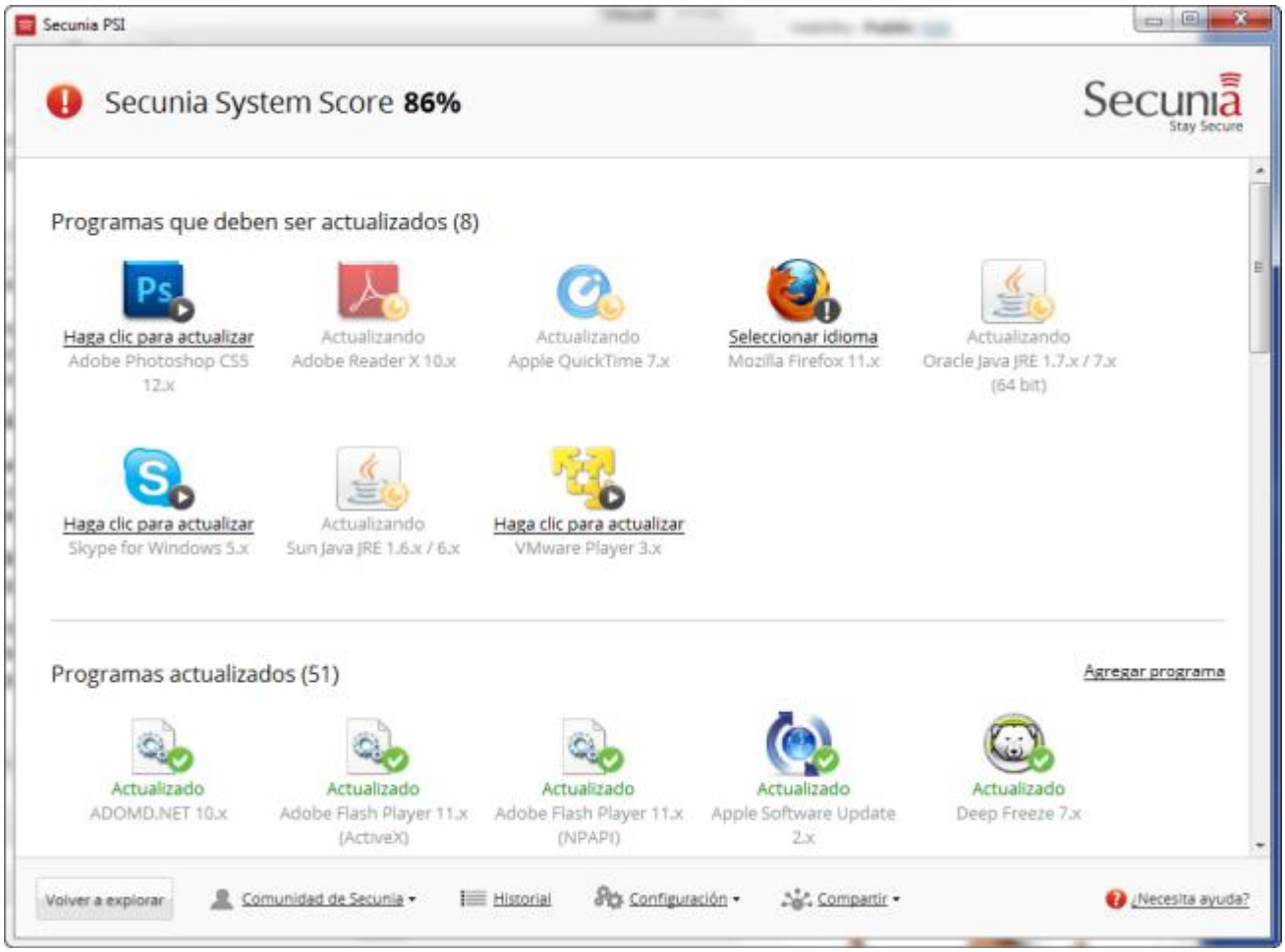
10 consejos de seguridad informática que debes seguir

http://articulos.softonic.com/10-consejos-de-seguridad-informatica-imprescindibles

Hay cosas que tu antivirus, por muy bueno que sea, no puede hacer. Te explico qué medidas de seguridad informática necesitas aplicar por tu cuenta.

1. Mantén actualizados los programas

Hay malware que se aprovecha de las vulnerabilidades en programas famosos para colarse en tu PC sin que el antivirus pueda actuar. Un ejemplo: el Virus de la Policía.



Para evitar sorpresas, debes **mantener actualizados tus programas**. Aplicaciones comoSecunia PSI o Softonic for Windows te ayudan a conseguirlo.

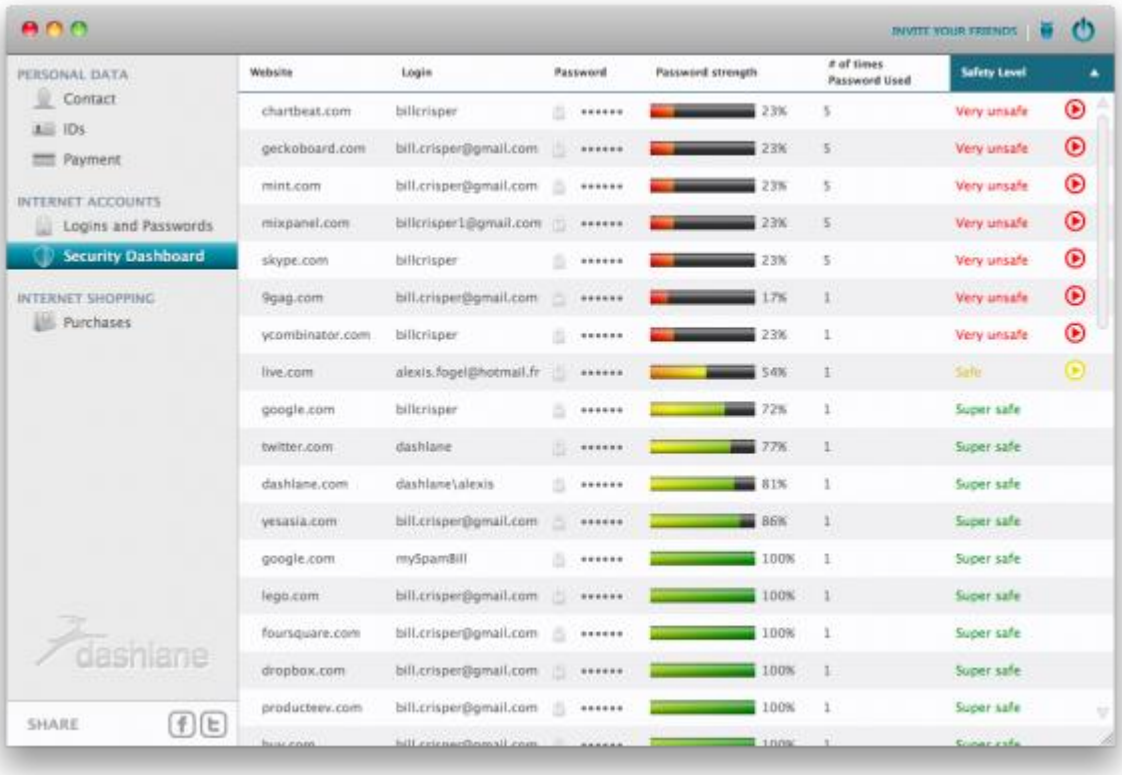
2. En redes públicas, navega con cifrado

En las redes WiFi públicas, tus datos pueden ser interceptados de muchas maneras. Navegar desde ellas sin protección es **una imprudencia que se paga muy cara**.

Para defenderte, navega siempre con el protocolo HTTPS activado; con HTTPS Everywherees muy fácil. Y para añadir seguridad extra, te recomiendo usar estas apps.

3. Crea usuarios y contraseñas distintos

Casi cada día aparecen noticias sobre contraseñas robadas en servicios importantes. El riesgo de que entren en tus cuentas una vez atacado un servicio es enorme.



Crea contraseñas distintas y seguras para todos tus servicios, y usa nombres de usuario diferentes cuando se te dé esa opción. Y usa un gestor de contraseñas como Dashlane.

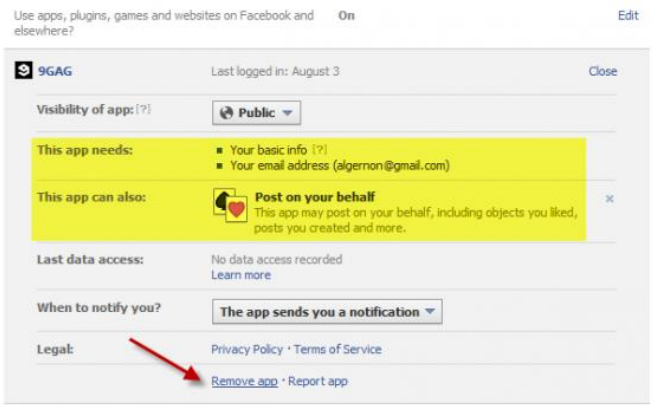
4. Cambia tus contraseñas a menudo

Las contraseñas envejecen. Y si las vulnera un intruso discreto, puede que tardes mucho en saber si alguien ha accedido a tus archivos y mensajes.

Por muy fuertes que sean tus contraseñas, **cámbialas periódicamente**. Y para añadir un factor de protección adicional, activa la verificación en dos pasos allá donde puedas.

5. Comprueba las apps autorizadas

"¿Puede la aplicación X leer tus datos de Facebook y Google?". Cuando autorizas una app maligna, el desastre está servido: **spam enviado en tu nombre, robo de datos**...

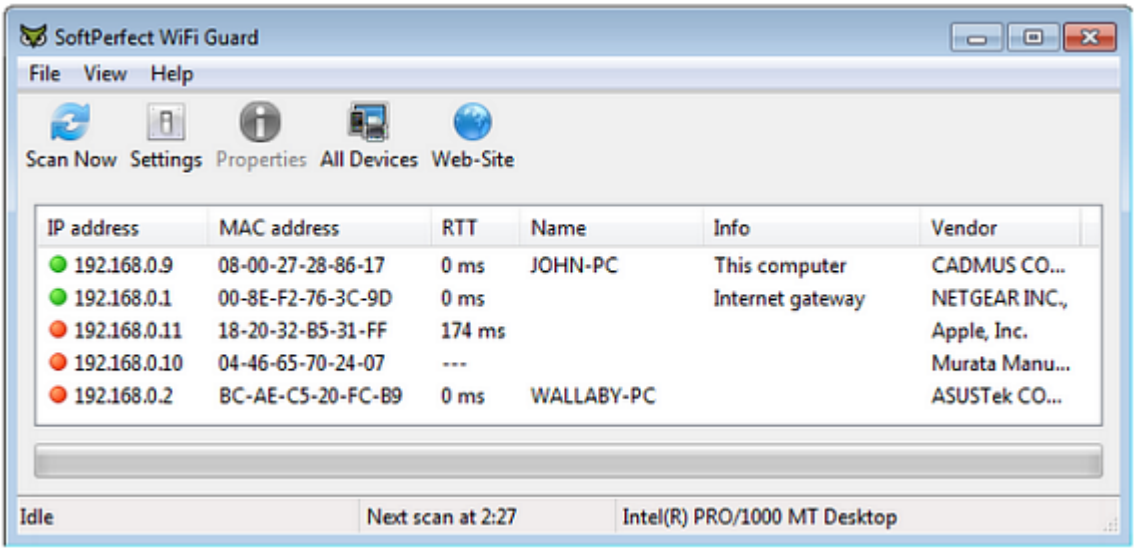


Revocando una aplicación en Facebook

Para prevenir problemas, controla las apps autorizadas de Google, Facebook, Twitter y otros sitios importantes. Revocar permisos es fácil y rápido.

6. Protege tu red WiFi frente a intrusos

Una red WiFi abierta es un gesto solidario... y peligroso. Un visitante mal intencionado puede intentar acceder a los datos de tu ordenador. Y entonces hablamos de intrusos.



Con SoftPerfect WiFi Guard puedes ver qué y quién está conectado a tu red WiFi

Revisar la seguridad de tu red WiFi es la mejor manera de evitar sorpresas desagradables. Sigue mis ocho consejos para reforzar tu red WiFi.

7. Controla la privacidad de tus redes

En tus perfiles de Facebook y Google hay un montón de información personal que **puede usarse en tu contra** (por ejemplo, para adivinar contraseñas).

Cuidado con los perfiles falsos en Facebook, podrían ser ladrones de datos...

Rechaza solicitudes de amistad sospechosas y configura bien la privacidad de Facebook yotras redes sociales. Es una cuestión de privacidad fundamental.

8. Crea usuarios para cada persona

He visto un montón de ordenadores con una sola cuenta para toda la familia. O con varias cuentas, pero desprotegidas. Es un camino seguro hacia el desastre.

Dos usuarios conviven en el mismo PC con Windows 7 (fuente)

Si más de una persona va a usar un PC, crea diferentes cuentas, cada una protegida por una contraseña fuerte u otro sistema de identificación. ¡Y por favor, bloquea el PC!

9. Desconfía de los archivos que te envían

Uno de los virus más dañinos de los últimos tiempos se propagó a través de Skype: un amigo enviaba un archivo y la gente, **al confiar en su origen**, lo abría. Y *kaputt*.

¿Vas a abrirlo aunque te lo haya enviado un amigo?

Estés donde estés, **no abras un archivo misterioso por ninguna razón**, ni siquiera si te lo envía un amigo. Pregúntale antes qué es. En la duda, escanéalo en la web.

10. Aprende a ser escéptico

La seguridad es una actitud. Implica desconfiar sanamente de las cosas que ves a diario en Internet, ese mágico mundo de colores... y estafas.

Sé escéptico. En mis guías Cómo detectar y desmontar bulos y Qué hacer ante un mail sospechoso te proporciono pautas de sentido común para ser más vigilante.