

Antivirus gratis: ¿cuál es el negocio?

Así hace dinero la Seguridad Informática que no cobra

Todos entendemos el **modelo de negocio del software**: pagás una licencia (o una cuota mensual) y tenés derecho a utilizar un programa. También entendemos que cuando un software o servicio online es gratuito, la empresa consigue ingresos de otra manera, por ejemplo, aprovechando nuestros datos. **Google y Facebook** son los reyes en esto.

¿Se traduce de la misma forma con los antivirus? En el caso de los antivirus de pago sí, porque simplemente pagás una suscripción o una licencia para poder utilizarlos en tu ordenador con Windows. Pero, ¿qué ocurre con los antivirus que son gratuitos? ¿cómo consiguen el dinero que necesitan para seguir funcionando?

El modelo "freemium" para aprovechar la atención de lo gratis

Una de las fórmulas que utilizan los antivirus gratuitos es, precisamente, amasar una buena comunidad de usuarios y aprovechar para **promocionarles una serie de servicios opcionales que cuestan dinero**. Sólo basta que cierta parte de esa comunidad acepte pagar y ya tenemos un negocio que se sostiene por sí mismo: en octubre, **Avast** se valuaba en dos mil millones de dólares.

Los responsables de **Avast Antivirus** lo describen así en su web oficial: tienen a más de 80 millones de usuarios que usan la base gratuita y que van recibiendo información sobre los planes de pago especializados con mejoras tanto para particulares como para empresas. Son esos usuarios de pago los que sostienen "*las nóminas, alquileres, costes de desarrollo y análisis de las amenazas nuevas que llegan a diario y el soporte de todos los usuarios*".

No obstante, eso no ha hecho que Avast **no haya tenido algún episodio controvertido**. Hace cuatro años la compañía tuvo que suspender la alianza con una empresa de terceros que se encargaba de su soporte técnico ya que aparecieron sospechas de que dicho soporte engañaba a los usuarios para que pagasen por una ayuda que no necesitaban. Afortunadamente el problema terminó allí y **Avast** no fue considerada responsable directa.

Bitdefender es otro ejemplo de este modelo *freemium*: un servicio básico gratuito para todo el mundo que sirve como base para ofrecer soluciones más completas de pago y conseguir así un grupo de suscriptores que mantengan el negocio.

Scareware, Adware y demás métodos "express" para conseguir ingresos

Lamentablemente, el modelo *freemium* **no se libra de tener prácticas que carecen de ética**. HowtoGeek tiene un "catálogo de los horrores" que nos lo demuestra: muchos programas de seguridad recurren a pequeños trucos como cambiarte el buscador configurado por defecto en tu navegador, instalarte esas horribles barras de herramientas que no sirven para nada en él, o instalar adware en forma de utilidades absurdas en el ordenador. Esto último suele hacerlo **AVG** en sus servicios gratuitos.

Avast también vuelve a convertirse en un ejemplo aquí: en octubre de 2014 la compañía fue acusada de utilizar adware para recopilar el historial de navegación de sus usuarios, cosa que el director de operaciones del programa desmintió en sus foros de soporte.

Avira quiere instalar extensiones de adware, **ZoneAlarm** quiere colocar su web oficial como página de inicio de tu navegador, **Panda Free** quiere colocar Yahoo como buscador por defecto en el navegador... todas las soluciones gratuitas tienen alguna que otra promoción. Cuando te ofrecen software legítimo no hay ningún problema, lo malo viene cuando lo que te instalás no tiene ninguna utilidad más que afectar el rendimiento de tu ordenador y colocarte más anuncios de la cuenta.

CONSEJOS

Muchas veces te preguntás si tal o cual antivirus es mejor o peor. Y más allá de que alguno puede tener mejor algoritmo de análisis, consumir más o menos recursos de tu computadora, lo importante es:

- ✓ **Mantené actualizado tu antivirus**
- ✓ **Revisá periódicamente tu disco duro completo**
- ✓ **Chequeá las memorias USB que fueras a conectar en tu computadora**

