Boletín mensual de consejos de seguridad para usuarios de computadoras

OUCH!

EN ESTA EDICIÓN...

- ¿Cómo funcionan los antivirus?
- ¿Qué hacen y qué no hacen para proteger tu equipo?
- Consejos para usar el antivirus
- Fuentes confiables para obtener antivirus

Conoce tu Antivirus

EDITOR INVITADO

Lenny Zeltser, nuestro editor invitado en este boletín OUCH!, dirige el equipo de consultoría de seguridad en Savvis (www.savvis.com) e imparte cursos de defensa contra malware (www.CombatingMalware.com) para el SANS Institute. Es usuario activo de Twitter en @lennyzeltser y regularmente escribe en su blog de seguridad blog.zeltser.com.

VISIÓN GENERAL

Cualquier computadora puede infectarse de malware. Malware es el término general que designa a todo programa malicioso tal como virus, gusano, caballo de Troya o programa espía (spyware), está diseñado para infectar y tomar el control de tu computadora. Una vez que tu computadora se infecta, los usuarios mal intencionados pueden capturar todo lo que escribes en el teclado, robar tus documentos y usar tu computadora para atacar a otras. El software antivirus busca proteger tu computadora contra el malware. El antivirus puede estar disponible como un producto independiente o incluirse en un paquete de software de seguridad.

El antivirus detecta y bloquea los intentos de los usuarios maliciosos para infectar tu computadora. El problema es que actualmente, el antivirus ya no puede mantener el mismo ritmo que los intrusos. Se liberan diariamente tantas versiones nuevas de malware que ningún antivirus puede detectar y protegerte de todas. Por esta razón, es posible que tu computadora se infecte aun teniendo instalada la última versión del antivirus. Para entender por qué pasa esto, revisemos cómo funcionan la mayoría de los antivirus.

DETECCIÓN DE FIRMA

La mayoría de los programas antivirus funcionan como el sistema inmunológico humano, buscando en tu computadora firmas (patrones o identificadores únicos) de agentes patógenos e infecciones digitales. Buscan en un diccionario de malware conocido y, si una parte de un archivo coincide con un patrón del diccionario, el software antivirus trata de neutralizarlo. Al igual que el sistema inmunológico humano, el diccionario requiere actualizarse, como al vacunarte contra la gripe, para brindar protección contra las nuevas cepas de malware. El antivirus sólo puede proteger de aquello que reconoce como amenaza. El problema es que aparece nuevo malware tan rápido, que los desarrolladores de antivirus no pueden seguirles el paso. Tu computadora es vulnerable durante el tiempo que transcurre entre la identificación de un nuevo malware

Conoce tu Antivirus

y la actualización del diccionario que realizan los fabricantes. Por esto es importante que mantengas tu antivirus actualizado en todo momento.

DETECCIÓN DE COMPORTAMIENTO

Con este enfoque, los antivirus no intentan identificar malware conocido, sino analizar el comportamiento del software instalado en tu computadora. Cuando un programa actúa de manera sospechosa, tal como tratar de acceder a un archivo protegido o modificar otro programa, el antivirus detecta esta actividad y envía una alerta. Este modo de detección brinda protección contra nuevos tipos de malware que todavía no existen en los diccionarios. Su inconveniente es que puede generar un gran número de falsas alarmas. Esto puede causar incertidumbre sobre qué permitir y qué no, y con el tiempo insensibilizarte a las advertencias. Incluso, podrías llegar a pasar por alto las advertencias dando clic en “Aceptar” en todas ellas, dejando tu computadora expuesta a infecciones y ataques.

CONSEJOS SOBRE ANTIVIRUS

1. No estás exento de riesgos

Cada computadora, sin importar su sistema operativo, es vulnerable a ataques. Aunque el antivirus no pueda proteger contra todos los tipos de malware, la seguridad de tu equipo es mucho mejor cuando instalas, mantienes actualizado y funciona correctamente un antivirus.

2. Descarga software sólo de fuentes confiables

Adquiere software antivirus sólo de distribuidores y fabricantes reconocidos y confiables. Es una táctica común de los ciber-delincuentes vender supuestos programas antivirus, que en realidad son malware. Al final de este boletín se listan algunas fuentes confiables de soluciones antivirus.

3. Mantén tu software actualizado

Asegúrate que tu computadora tenga instalada la última versión del antivirus y que esté configurada para

¡Importante! Siempre mantén tu antivirus actualizado.

Conoce tu Antivirus

actualizarse automáticamente. Verifica periódicamente que las firmas estén actualizadas.

4. No postergues las actualizaciones

Si tu computadora estuvo apagada o sin conexión durante algún periodo de tiempo, al prenderla o conectarla a Internet, tu antivirus necesitará actualizarse. No pospongas estas actualizaciones, ya que son indispensables.

5. Analiza todos tus dispositivos

Verifica que tu antivirus revise dispositivos extraíbles, como memorias USB, cuando los conectes a tu computadora.

6. Atiende advertencias y alertas

Presta atención a todas las alertas generadas por el antivirus. La mayoría de las alertas incluyen la opción de seguir un enlace para obtener más información o recomendaciones sobre qué hacer. Si es la computadora del trabajo, registra el mensaje de alerta y contacta al soporte técnico o equipo de seguridad.

7. Nunca desactives tu antivirus

No deshabilites el software de seguridad porque creas que haga más lenta tu computadora, te bloquee una página web o te prevenga de instalar una aplicación o programa. Si haces esto, expondrás tu computadora a riesgos innecesarios que podrían resultar en incidentes serios de seguridad. Si los problemas persisten, sustituye tu antivirus por otro.

8. Instala sólo un antivirus

No instales más de un programa antivirus al mismo tiempo, ya que podría interferir uno con la operación del otro, dejando tu computadora con menos protección en vez de tener más.

9. Considera un kit completo de seguridad

Debes estar consciente que el antivirus no protegerá tu computadora contra todas las amenazas. Te recomendamos instalar una solución de seguridad que incluya herramientas adicionales como un firewall, protección para el navegador y otras funciones avanzadas.

FUENTES CONFIABLES PARA OBTENER ANTIVIRUS

Consumer Reports – http://preview.tinyurl.com/5ve99ck

Usuario Casero – http://preview.tinyurl.com/48ycdlp

APRENDE MÁS

Suscríbete al boletín mensual *OUCH!* El boletín de conciencia sobre seguridad. Accede a los archivos de *OUCH!*, y aprende más acerca de las soluciones preventivas de seguridad que SANS tiene para ti. Visítanos en: http://www.securingthehuman.org.

VERSIÓN EN ESPAÑOL

UNAM-CERT, único equipo de respuesta a incidentes en México reconocido ante FIRST, es una referencia en seguridad de la información en este país. Sitio web http://www.seguridad.unam.mx, síguelo en Twitter: @unamcert.

Consejo Editorial: Bill Wyman, Walt Scrivens, Phil Hoffman, Lance Spitzner, Carmen Ruyle Hardy
Versión en español a cargo de UNAM-CERT: Cecila Espinosa, Israel Andrade, Galvy Cruz, Mauricio Andrade, Rubén Aquino