Parches o updates.

Un parche consta de cambios que se aplican a un programa, para corregir errores, agregarle funcionalidades, actualizarlo, modificar su apariencia o rendimiento, etc.

Un parche puede ser aplicado tanto a un binario ejecutable como al código fuente de cualquier tipo de programa, incluso, un sistema operativo.

El origen del nombre probablemente se deba a la utilidad de Unix llamada patch creada por Larry Wall.

Los parches reparan huecos de seguridad en los programas o sistemas operativos, por lo cual son un elemento esencial para que una aplicación o el propio sistema funcione adecuadamente.

Las actualizaciones tienen como objetivo reparar problemas específicos de vulnerabilidades que se presentan en un programa. Algunas veces, en lugar de liberar un sólo parche o actualización, los distribuidores publican una versión actualizada de su software, aunque podrían referirse a ésta como un parche.

El tamaño de los parches es variable. Algunos parches solamente modifican un archivo binario de la aplicación pero otros alteran mucho más el contenido. Si el parche sólo modifica el ejecutable, puede ser muy pequeño por debajo del megabyte. La instalación de parches solía ser una tarea tediosa, y con mucha posibilidad de error. Un error solía significar tener que reinstalar la aplicación y el parche. Hoy en día, la instalación de parches se realiza, en muchos casos, por programas especiales de forma automática.

Algunos programas pueden actualizarse automáticamente por medio de Internet con muy poca o nula intervención del usuario. Es muy popular que el mantenimiento de los sistemas operativos se haga de esta manera. En situaciones donde los administradores de sistemas controlan un cierto número de computadoras, esta manera de automatización ayuda a mantener la consistencia. La aplicación de parches de seguridad comúnmente ocurre de esta forma.

Cuando las actualizaciones están disponibles, los distribuidores usualmente las liberan a través de sus sitios web para que los usuarios las descarguen. Algunos programas cuentan con herramientas de actualización automática cada vez que existe algún parche disponible, tal es el caso de Windows Update. Es importante instalar las actualizaciones tan pronto como sea posible para proteger al

equipo de los intrusos, quienes buscan tomar ventaja de las vulnerabilidades. Si estas opciones automáticas están disponibles, es recomendable aprovecharlas, si no lo están, se aconseja verificar los sitios web de su distribuidor periódicamente en busca de actualizaciones.

Asegúrate de descargar software o actualizaciones sólo desde sitios web confiables, nunca lo hagas a través de enlaces que aparezcan en mensajes de correo electrónico, pues los intrusos acostumbran hacer que los usuarios visiten sitios web que inyectan o propagan códigos maliciosos disfrazados de actualizaciones. También, ten cuidado con los mensajes de correo electrónico en los que se afirme que un archivo adjunto es una actualización de software, estos archivos adjuntos comúnmente son virus.

El sistema iOS no incluye una herramienta de actualización automática, el usuario debe revisar, descargar y aplicar las actualizaciones utilizando iTunes, en el caso de Android algunas versiones pueden actualizar el software mas no las aplicaciones ya que al ser un sistema operativo de código abierto, las aplicaciones dependen de terceros para aplicar parches o actualizaciones a dichas aplicaciones, se puede configurar para que las actualizaciones sean descargadas de manera automática sin embargo algunas requieren permiso del usuario para ser aplicadas.

Comprobar si la tienda es real, leer las condiciones generales o no hacer transacciones bancarias sin cifrar son algunas de las claves para evitar la estafa online. Las recomendaciones mencionadas: son: