1. HERRAMIENTAS PARA PROTEGER NUESTRO ORDENADOR

En la primera parte de esta unidad nos hemos familiarizado con las amenazas que circulan por la red global, y que ponen en riesgo la integridad de nuestros equipos informáticos. Para proteger nuestros ordenadores, necesitaremos utilizar una serie de herramientas básicas. Es fundamental te familiarices con éstas, y que las instales y mantengas actualizadas, para evitar que el malware pueda tener acceso.

Las tres herramientas básicas de protección – a veces integradas en un mismo programa- son: Antivirus, Antispyware (Antiespías) y Firewall (Cortafuegos).

Veamos en detalle cada uno de estos útiles

1.1. ANTIVIRUS

Son programas diseñados para detectar, bloquear y/o eliminar el software dañino. Tienen dos mecanismos básicos de detección de amenazas:

1. Comparación, buscando entre los programas el patrón de código que coincida con los almacenados en una biblioteca de patrones de virus conocidos.
2. Detección de programas hostiles basados en su comportamiento. El antivirus conoce una serie de comportamientos sospechosos y estudia a los programas que, por su código, estén preparados para llevarlos a cabo.

Es importantísimo que tengas instalado en tu ordenador un antivirus. Estos paquetes son algo parecido a nuestros guardaespaldas; se mantienen siempre alerta de posibles programas dañinos que puedan colarse en tu ordenador y hacer uso de los datos y archivos que tienes guardados. Por ello es básico que tengas instalado un antivirus. Además preocúpate de actualizarlo cada cierto tiempo, ya cada día aparecen nuevos virus, y si no tienes las últimas "vacunas" serás vulnerable a sus ataques.

1.2. ANTISPYWARE (ANTIESPÍAS)

Son aplicaciones que se encargan de que en tu ordenador no haya programas que roben tus datos.

Aunque hoy en día los antivirus tratan de ampliar su protección hacia cualquier tipo de malware, y suelen incluir esta función, en ocasiones es necesario utilizar programas específicos para detectar el spyware, que complementan la actividad del antivirus.

Por otro lado, la mejor manera de protegerse de los programas hostiles es ser consciente de su existencia y hacer un uso de la red y del software que minimice el riesgo de que puedan entrar en el sistema. La prudencia es la principal herramienta y se ha de extremar la cautela a la hora de enfrentarse a un programa desconocido. No todos los programas que se reciben por correo o se descargan gratuitos de la red están limpios de amenazas. Es importante comprobar y pensar antes de ejecutar.

1.3. FIREWALL (CORTAFUEGOS)

Un cortafuegos o firewall es un elemento encargado de controlar y filtrar las conexiones a red de una máquina o conjunto de máquinas. Se trata de un mecanismo básico de prevención contra amenazas de intrusión externa. Supone la barrera de protección entre un equipo o red privada y el mundo exterior. Controla el acceso de entrada y salida al exterior, filtra las comunicaciones, registra los eventos y genera alarmas.

Este tipo de programas son como el portero de tu ordenador: nadie pasará sin que él les dé permiso para hacerlo. Te avisa de posibles programas que quieren hacer algo malo en tu ordenador y te hacen invisible ante los posibles ladrones en busca de víctimas. En algunas páginas web encontraras descargas gratuitas de cortafuegos y es recomendable que te hagas con uno de estos "porteros".

Puedes visitar la siguiente web para ver una Infografía interesante para comprender mejor el funcionamiento de un Firewall (Link).

EJERCICIOS

1. Busca en Internet 5 software antivirus de reconocido prestigio. ¿Qué precio tendría para un usuario particular comprar uno de estos antivirus?
2. Encuentra 3 antivirus gratuitos en la red. ¿Incluyen Antispyware o Firewall entre sus funcionalidades?
3. Una vez comprado un antivirus, ¿se puede seguir utilizando durante tiempo ilimitado? ¿Por qué?
4. Visita las siguientes webs e indica en un párrafo en qué consiste cada una de ellas:
http://www.osi.es/
http://cert.inteco.es/
5. Busca en la Wikipedia información sobre el programa Spybot-Search & Destroy. ¿Para qué sirve? ¿Quién lo creó? ¿Cuánto cuesta?
6. Si en una página web encuentras disponible un Antispyware gratuito que dice detectar amenazas graves presentes en tu PC ¿Crees que sería conveniente descargarlo e instalarlo? Justifica tu respuesta.
7. Dí si la siguiente frase es Verdadera o Falsa, y justifica tu respuesta: "Internet es la principal fuente de amenazas para la seguridad de un ordenador y, sin embargo disponer de conexión a Internet puede llegar a ser la mejor manera para protegernos".
8. Investiga cómo se configura el Firewall que viene incluido en el Sistema Operativo Windows. Explica para qué crees que sirven las Excepciones del Firewall.