1. Protección del ordenador. Consejos técnicos

Internet tiene muchísimas ventajas pero también está lleno de peligros y riesgos. Cuando salimos a la calle estamos atentos de que no nos quiten o se nos pierdan nuestras carteras o monederos donde llevamos toda nuestra documentación, todos esos datos que nos identifican, como el DNI, nuestras fotos, esa entrada de tu concierto favorito, en definitiva protegemos nuestra intimidad. ¿Por qué no hacemos lo mismo en Internet? En la tranquilidad de nuestras habitaciones nos creemos a salvo del mundo, pero en el momento en el que nuestro ordenador se conecta a la telaraña mundial, que es Internet, estamos totalmente desprotegidos, expuestos a millones de riesgos que nos traerán consecuencias graves si no tomamos las medidas oportunas. Lo mismo ocurre con cualquier sistema informático móvil o portátil.

1.1. Máquinas de clasificar y registrar operaciones

Los sistemas informáticos registran todo, guardan todas las páginas web que has visitado, las películas, o la música que has descargado, las búsquedas que has hecho en Google o Yahoo, tu correo electrónico, los datos que has rellenado en algún formulario de inscripción, tus contraseñas, tus conversaciones de mensajería instantánea..., todo. Nunca olvida nada a no ser que tú se lo digas explícitamente y lo peor de todo: cualquiera que tenga unos conocimientos mínimos de informática podrá saberlo todo sobre ti y utilizar tus datos de forma inadecuada. Pero vamos por partes; cualquier sistema informático lo tiene todo clasificado y guardado en distintos lugares, antes de darte algunos consejos informáticos para estar protegido de los ladrones de datos veamos que se guarda en cada sitio:

• Historial: Aquí se almacenan la gran mayoría de las páginas web que has visitado. Son algunas de las “huellas” que vas dejando por la Red, así que conviene borrarlas para que nadie las siga.

• Cookies (huellas): Son archivos que contienen la dirección de la página que acabas de visitar. Algunas son temporales, pero otras pueden permanecer en tu ordenador durante años. Los espías pueden hacer un seguimiento de las páginas web que has visitado y acceder a tus archivos, de esta manera sabrán tus gustos y preferencias; con ello crean listas de posibles clientes que luego venden a empresas comerciales. Es importante que cada cierto tiempo las elimines.

• Archivos: Las imágenes y contenidos de las páginas web que has visitado se almacenan en nuestro ordenador para así acelerar la carga de la página cuando vuelvas a visitarla. Pero a partir de estos archivos se puede acceder a los datos que has escrito en

las páginas web que has visitado. Al borrar estos archivos tardará un poco más en cargarse la página pero estarás protegido de los espías y ladrones informáticos.
Ahora que ya sabes que guarda tu ordenador y donde lo guarda, te aconsejamos que cada cierto tiempo, al menos cada semana dediques cinco minutos a borrar todos estos datos que se quedan en tu ordenador y evitar que los ladrones de datos invadan tu intimidad. ¿Cómo? Realiza la siguiente actividad:

Abre un navegador de internet, e investiga cómo se eliminan el Historial, las Cookies y los archivos temporales. Escribe detalladamente la secuencia de pasos a seguir para conseguirlo:

2. Ataques de virus (y otros)

Ahora ya sabes un poco más sobre un sistema informático, pero todavía no estas a salvo y tienes una nueva misión: no dejar que se convierta en un zombi manejado por extraños y protegerle de todos los peligros que existen en Internet. ¿Todavía no sabes los nombres de estos atacantes? Hay una plaga de ellos en Internet y aunque te sorprenda saberlo, también en el teléfono móvil. Son programas informáticos que se propagan con muchísima facilidad y son muy dañinos. A veces se manifiestan y sabemos que están ahí pero otras muchas se esconden en archivos o programas que nos descargamos pudiendo con ello destruir los datos de tu ordenador, sustraer tus datos personales, tus fotos... En definitiva manejando tu ordenador por ti, convirtiéndolo en un zombi.

A continuación te damos toda la información que necesitas sobre estos malhechores y los escudos para estar protegidos:

¿Qué son los virus?

Los virus son programas maliciosos creados para manipular el normal funcionamiento de los sistemas, sin el conocimiento ni consentimiento de los usuarios.

Actualmente, por sencillez, el término virus es ampliamente utilizado para referirse genéricamente a todos los programas que infectan un sistema, aunque en realidad, los virus son sólo un tipo específico de este tipo de programas. Para referirse a todos ellos también se suelen emplear las palabras “malware” que procede de las siglas en inglés malicious software.

Los programas maliciosos pueden alterar tanto el funcionamiento del equipo como la

información que contienen o se maneja en ella. Las acciones realizadas en la máquina pueden variar desde el robo de información sensible o el borrado de datos hasta el uso del equipo como plataforma para cometer otro tipo de actividades ilegales –como es el caso de las redes zombies-, pudiendo llegar incluso a tener sus respectivas consecuencias legales.

En sus comienzos la motivación principal para los creadores de virus era la del reconocimiento público. Cuanta más relevancia tuviera el virus, más reconocimiento obtenía su creador. Por este motivo las acciones a realizar por el virus debían ser visibles por el usuario y suficientemente dañinas como para tener relevancia, por ejemplo, eliminar ficheros importantes, modificar los caracteres de escritura, formatear el disco duro, etc.

Sin embargo, la evolución de las tecnologías de la comunicación y su penetración en casi todos los aspectos de la vida diaria ha sido vista por los ciberdelincuentes como un negocio muy lucrativo. Los creadores de virus han pasado a tener una motivación económica, por lo que actualmente son grupos mucho más organizados que desarrollan los códigos maliciosos con la intención de que pasen lo más desapercibidos posibles, y dispongan de más tiempo para desarrollar sus actividades maliciosas.

Investigar sobre el virus de la policía

¿A qué afectan los códigos maliciosos o malware?

Los programas maliciosos afectan a cualquier dispositivo que tenga un Sistema Operativo, es decir: Ordenadores personales, Servidores, Teléfonos Móviles, Videoconsolas, …

¿Por qué hay gente que crea programas maliciosos?

Cuando surgieron los primeros virus y programas maliciosos solía ser muy sencillo darse cuenta de que el ordenador estaba infectado, ya que los virus generalmente realizaban alguna acción visible en el equipo, por ejemplo, borrar ficheros, formatear el disco duro, cambiar los caracteres de escritura, etc.

Actualmente los programas maliciosos han evolucionado y suelen perseguir un fin lucrativo. Para lograr más fácilmente su cometido suelen pasar desapercibidos para el usuario, por lo que son más difíciles de detectar de forma sencilla. Hay varias formas en las que el creador del programa malicioso puede obtener un beneficio económico, las más comunes son:

- Robar información sensible del sistema infectado, como datos personales,

contraseñas, credenciales de acceso a diferentes entidades...

- Crear una red de sistemas infectados -generalmente llamada red

  zombie o botnet- para que el atacante pueda manipularlos todos simultáneamente y vender estos servicios a entidades sin escrúpulos que puedan realizar acciones poco legítimas como el envío de SPAM, envío de mensajes de phishing, realizar ataques de denegación de servicio, etc.
- Vender falsas soluciones de seguridad que no realizan las acciones que afirman hacer, por ejemplo, falsos antivirus que muestran mensajes con publicidad informando de que el ordenador está infectado cuando en realidad no es así, la infección que tiene el usuario es el falso antivirus.
- Cifrar el contenido de los ficheros del ordenador y solicitar un “rescate” al usuario del equipo para recuperar la información, como hacen los criptovirus.

2.1. Tipos de virus

Los distintos códigos maliciosos que existen pueden clasificarse en función de diferentes criterios, los más comunes son:

- por su capacidad de propagación
- por las acciones que realizan en el equipo infectado.

Algunos de los programas maliciosos tienen alguna característica particular por la que se les suele asociar a un tipo concreto mientras que a otros se les suele incluir dentro de varios grupos a la vez. También cabe mencionar que muchas de las acciones que realizan los códigos maliciosos, en algunas circunstancias se pueden considerar legítimas, por lo tanto, como dijimos anteriormente, sólo se considera que un programa es malicioso cuando actúa sin el conocimiento ni consentimiento del usuario.

Los posibles tipos de virus y sus clasificaciones son los siguientes:

Según su capacidad de propagación

Atendiendo a su capacidad de propagación, o mejor dicho de autopropagación, existen tres tipos de códigos maliciosos:

• **Virus**: Su nombre es una analogía a los virus reales ya que infectan otros archivos, es decir, sólo pueden existir en un equipo dentro de otro fichero. Los ficheros infectados generalmente son ejecutables: .exe, .src, o en versiones antiguas .com, .bat; pero también pueden infectar otros archivos, por ejemplo, un virus de Macro infectará programas que utilicen macros, como los

productos Office.

Los virus se ejecutan cuando se ejecuta el fichero infectado, aunque algunos de ellos además están preparados para activarse sólo cuando se cumple una determinada condición, por ejemplo que sea una fecha concreta. Cuando están en ejecución, suelen infectar otros ficheros con las mismas características que el fichero anfitrión original. Si el fichero que infectan se encuentra dentro de un dispositivo extraíble o una unidad de red, cada vez que un nuevo usuario acceda al fichero infectado, su equipo también se verá comprometido.

Los virus fueron el primer tipo de código malicioso que surgió, aunque actualmente casi no se encuentran nuevos virus pasando a hallarse en los equipos otros tipos de códigos maliciosos, como los gusanos y troyanos que se explican a continuación.

• Gusanos: Son programas cuya característica principal es realizar el máximo número de copias de sí mismos posible para facilitar su propagación. A diferencia de los virus no infectan métodos:

- Correo electrónico
- Redes de compartición de ficheros (P2P) o Explotando alguna vulnerabilidad
- Mensajería instantánea
- Canales de chat

Generalmente los gusanos utilizan la ingeniería social para incitar al usuario receptor a que abra o utilice determinado fichero que contiene la copia del gusano. De este modo, si el gusano se propaga mediante redes P2P, las copias del gusano suelen tener un nombre sugerente de, por ejemplo, alguna película de actualidad; para los gusanos que se propagan por correo, el asunto y el adjunto del correo suelen ser llamativos para incitar al usuario a que ejecute la copia del gusano.

Eliminar un gusano de un ordenador suele ser más fácil que eliminar un virus. Al no infectar ficheros la limpieza del código malicioso es más sencilla, no es necesario quitar sólo algunas partes del mismo basta con eliminar el archivo en cuestión.

Por otro lado, como los gusanos no infectan ficheros, para garantizar su autoejecución suelen modificar ciertos parámetros del sistema, por ejemplo, pueden cambiar la carpeta de inicio con el listado de todos los programas que se tienen que ejecutar al arrancar el ordenador, para incluir en el listado la copia del gusano; o modificar alguna clave del registro que sirva para ejecutar programas en determinado momento, al arrancar el ordenador, cuando se llama a otro programa...

• Troyanos: Carecen de rutina propia de propagación, pueden llegar al sistema de diferentes formas, las más comunes son:

o Descargado por otro programa malicioso.
o Descargado sin el conocimiento del usuario al visitar una página web maliciosa.
o Dentro de otro programa que simula ser inofensivo.

Cómo llegan al sistema y cómo prevenirlos

Existen gran variedad de formas por las que los virus, gusanos y troyanos pueden llegar a un ordenador; en la mayoría de los casos prevenir la infección resulta relativamente fácil siguiendo unas sencillas pautas. Las formas en que un programa puede llegar al ordenador son las siguientes:

- Explotando una vulnerabilidad: cualquier programa del ordenador puede tener una vulnerabilidad que puede ser aprovechada para introducir programas maliciosos en el ordenador. Es decir, todos los programas que haya instalados en el equipo, ya sean: Sistemas Operativos -Windows, Linux, OS X, iOS, Android, etc-, navegadores Web -Internet Explorer, Firefox, Opera, Chrome, Safari, etc-, o cualquier otra aplicación –reproductores multimedia, programas de ofimática, compresores de ficheros, etc-, es posible que tengan alguna vulnerabilidad que sea aprovechada por un atacante para introducir programas maliciosos. Para prevenir quedarse infectado de esta forma, recomendamos tener siempre actualizado el software el equipo.
- Ingeniería social: apoyado en técnicas de ingeniería social para apremiar al usuario a que realice determinada acción. La ingeniería social se utiliza sobre todo en correos de phishing, pero puede ser utilizada de más formas, por ejemplo, informando de una falsa noticia de gran impacto, un ejemplo puede ser alertar del comienzo de una falsa guerra incluyendo un enlace en que se puede ver más detalles de la noticia; a donde realmente dirige el enlace es a una página Web con contenido malicioso. Tanto para los correos de phishing como para el resto de mensajes con contenido generado con ingeniería social, lo más importante es no hacer caso de correos recibidos de remitentes desconocidos y tener en cuenta que su banco nunca le va a pedir sus datos bancarios por correo.
- Por un archivo malicioso: esta es la forma que tienen gran cantidad de troyanos de llegar al equipo. El archivo malicioso puede llegar como adjunto de un mensaje, por redes P2P, como enlace a un fichero que se encuentre en Internet, a través de carpetas compartidas en las que el gusano haya dejado una copia de sí mismo...La mejor forma de prevenir la infección es analizar con un antivirus

actualizado todos los archivos antes de ejecutarlos, a parte de no descargar archivos de fuentes que no sean fiables.

- Dispositivos extraíbles: muchos gusanos suelen dejar copias de sí mismos en dispositivos extraíbles para que automáticamente, cuando el dispositivo se conecte a un ordenador, ejecutarse e infectar el nuevo equipo. La mejor forma de evitar quedarse infectados de esta manera, es deshabilitar el autoarranque de los dispositivos que se conecten al ordenador.

3. Herramientas para defender un sistema informático

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 sistemas, 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

3.1. 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.

3.2. Antispyware (Anti espía)

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 qu 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.

3.3. 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”.