IES CAMPOS Y TOROZOS. DPTO. TECNOLOGÍA

INFORMÁTICA 4º ESO

UNIDAD1: CUIDADO CON EL MALWARE!!!:

Como todos sabemos Internet está aumentando cada vez más su influencia en nuestra forma de vida, ya no solo es un sitio donde **buscar información**, se ha convertido en una herramienta que nos permite en muchas ocasiones **ahorrar tiempo** (podemos realizar tramites administrativos, bancarios,....) **y dinero** (artículos en Internet pueden ser más baratos), además cada vez utilizamos mucho más Internet para ampliar **nuestras relaciones personales**.

Pues bien, en la actualidad el menor **peligro** de navegar por Internet es que se nos cuele un virus en el ordenador que nos **estropee el ordenador**, ya que sin saberlo en todas las actividades que realizamos en la red vamos dejando nuestro rastro en la red y sino tenemos cuidado **nuestros datos personales** (dirección de correo, número de cuenta, contraseñas,....) pueden caer **en malas manos**.

En las siguientes páginas estudiaremos cuales son los **principales peligros a los que nos enfrentamos al navegar por Internet**, representados por el **MALWARE**, que es el software que tiene como objetivo infiltrarse en el ordenador sin el conocimiento de su dueño y con finalidades muy diversas que pueden ir desde mostrarnos publicidad, bloquearnos el ordenador, dañar archivos, robarnos datos,.....Aquí tenemos el guión.

1.- Virus.

2.- Troyanos.

3.- Gusanos.4.- Spyware.

5.- Phishing y Pharming.

6.- Spam.

1.- LOS VIRUS:

Los virus **son programas** de ordenador como el Word o el Photoshop, pero en vez de estar diseñados para hacer algo útil han sido **concebidos para dañar los sistemas informáticos** en mayor o menor medida.

Estos programas tienen la siguiente **estructura**:

- El **módulo de reproducción:** Es la parte del programa que permite al virus copiarse en ciertos archivos, e infectar a nuevos ordenadores.

-El **módulo de ataque**: Es el que realmente provoca el daño.

-El **módulo de defensa** tiene, obviamente, la misión de proteger al virus retrasando en lo posible su detección y eliminación.

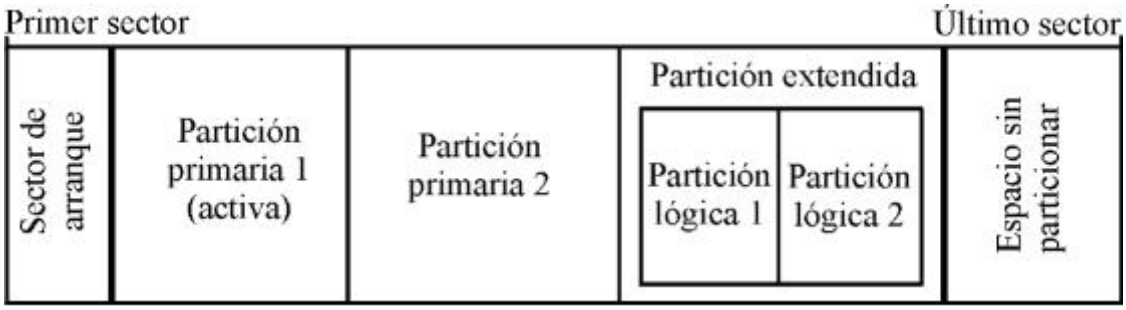
¿Que daños puede provocar un virus?:

Al igual que los virus que entran en nuestro organismo se especializan en atacar un tipo determinado de células, **cada virus** informático **se especializa en copiarse en un tipo determinado de archivos**, en función de la importancia de dichos archivos los daños pueden ser más o menos importantes:

- **Puede que el virus sea benigno**, es decir, que ni siquiera tenga un módulo de ataque o se que se limite a mostrar un mensaje que deja patente su presencia en el sistema.

- **Puede que infecte a archivos ejecutables**, es decir, los que nos sirven para abrir programas como el word, paint,...., de esta forma nos quedaríamos sin poder utilizar dichos programas. Ahora bien, no todos los programas en el ordenador son igual de importantes, por ejemplo, hay programas que sino se ejecutan pueden provocar que el ordenador se nos reinicie continuamente, se nos quede bloqueado, que vaya muy lento,.....

- Hay virus que se especializan en **infectar las partes del disco duro que intervienen en el arranque del ordenador**. Observa la siguiente imagen:



Esta imagen representa la estructura de un disco duro, la cual contiene cuatro particiones y un sector de arranque. Pasamos a explicar que es el sector de arranque: Es una pequeña región del disco duro en la que **se encuentra un fichero denominado MBR** (Master Boot Record). Dicho fichero que encarga de:

- Cuando arranca el ordenador **analiza la tabla de particiones** que se encuentra también en el sector de arranque, es decir, cuantas particiones hay (en nuestro caso cuatro), de que tipo (primarias, extendidas o lógicas), donde empiezan y donde terminan las particiones,....

- **Identifica en que parte del disco duro** se encuentra la partición activa, o lo que es igual, la partición en la que **hemos instalado el sistema operativo** Windows XP, Vista, Ubuntu,...

- Y por último, el fichero MBR **cede el control a la partición activa** donde está instalado el sistema operativo, a partir de ese momento **se empieza a encender en ordenador**.

Como puedes comprender si el virus altera el contenido del fichero MBR, de la tabla de partición, o de cualquier otro archivo que interviene en esta cadena, el sistema no será capaz de encontrar al sistema operativo y por lo tanto no podrá arrancar. Por esta razón es muy recomendable tener una copia de

seguridad de la tabla de partición que puede ser almacenada en un disquete o un CD.

- **Hay virus que infectan la BIOS**, es decir, el software que instala el fabricante del ordenador para que entre otras cosas se puedan entender entre si todos los dispositivos de hardware que se encuentran instalados en el ordenador (microprocesador, memoria, tarjeta gráfica, teclado,...). Por lo tanto, si la BIOS falla el ordenador no puede realizar ningún trabajo.

2.- TROYANOS:

Se denomina troyano a un programa malicioso **capaz de alojarse en computadoras y permitir el acceso a usuarios externos**, a través de una red local o de Internet, con el fin de **recabar información o controlar remotamente a la máquina** anfitriona.

La diferencia fundamental entre un troyano y un virus consiste en su finalidad, al contrario que un virus, el troyano no necesariamente provoca daños porque no es su objetivo.

Suele ser un programa alojado dentro de una aplicación, y se instala en el sistema al ejecutar dicha aplicación. Una vez instalado parece realizar una función útil, pero internamente realizan otras tareas de las que el usuario no es consciente, por ejemplo **puede ser utilizado para**:

- **Tomar el control total de la máquina**, es decir, pueden introducir todos los archivos que quieran en nuestro ordenador (entre ellos virus), desactivar el antivirus o el cortafuegos, el pirata informático se podrá conectar a través de nuestro ordenador a un módem de alto coste que por ejemplo ofrezca servicios de pornografía y endosarnos la factura, o establecer una contraseña para el usuario administrador de tu ordenador, de forma que no puedas acceder a tu propio equipo,

- **Enviar masivamente** correo electrónico no deseado (**spam**)

- Realizar **ataques a terceros**.

- **Diseminar virus** informáticos.

- Para **capturar datos** (contraseñas y claves de acceso) ya que pueden controlar las pulsaciones del teclado cuando escribimos las contraseñas. En este caso, se utilizaría como espía.

- Para realizar **cualquier otro delito informático**, y ocultar su identidad.

3.- GUSANOS:

Son programas "Malware" que **suelen acompañar a un correo electrónico como archivo adjunto** (aunque no siempre).

Una vez que el incauto usuario abre el archivo adjunto el gusano informático se copia en algún directorio del ordenador y empieza a hacer sus fechorías, **entre otras cosas puede provocar**:

1. La característica fundamental de este tipo de software es que puede **hacer copias de si mismo** en el propio ordenador, **para ello identifica los ficheros con ciertas extensiones** (vbs, css, jpg, mp3,....) **los borra** y a continuación **copia las líneas del programa del gusano** en dichos archivos.

Por lo tanto, la primera consecuencia es que en poco tiempo podemos tener cientos de archivos borrados del ordenador, y sustituidos por cientos de archivos gusanos. Tal vez nos hemos quedado sin canciones o fotos, o tal vez nuestro ordenador no funcione. Imagina que el artista que diseña el gusano decide que este se reescriba en los archivos .mp3, y que eres usuario de algún programa P2P como por ejemplo Ares o Emule, ¿Aciertas a adivinar las consecuencias?.

2. Otra característica de este tipo de software malicioso es que **puede copiarse entre nodos de una red de forma automática**. Por ejemplo, en una red local como la de nuestro aula cada ordenador es un nodo, y en Internet cada servidor es un nodo.

Por lo tanto, si tengo una red local de ordenadores y están infectados, estos no se podrían conectar a Internet ya que estarían demasiado ocupados mandándose gusanos unos a otros (se consumiría el ancho de banda).

3. Algo que suelen tener en común los gusanos es que **se hacen con la libreta de direcciones de correo** de la víctima (las que tenemos en Outlook, MNS Messenger,....) y automáticamente mandan un mensaje de correo a todas estas direcciones **con el fin de infectar también a más equipos**. Como podrás comprender uno de los mayores peligros de este tipo de Malware es que su velocidad de propagación es enorme, cuando se quiere lanzar la alerta de que ha aparecido un nuevo gusano y se incluye en las bases de datos de los antivirus ya puede ser demasiado tarde.

5. También **puede conectarse a algún servidor de Internet y descargar** cualquier otro tipo de software mal intencionado, **por ejemplo, un troyano**. De esta forma, estaríamos uniendo la gran capacidad de reproducirse y propagarse de los gusanos con la enorme peligrosidad y poder de devastación de otros virus y troyanos.

6. Existen incluso **algunos** gusanos que se encuentran **diseñados especialmente para transmitirse por Bluetooth**, infectando rápidamente a los teléfonos móviles, PDA u otros dispositivos que utilizan esta tecnología y que se encuentran en el radio de acción del teléfono afectado y que acepten la transmisión.

4.- SPYWARE:

El Spyware es un software que una vez introducido en el ordenador r**ealiza un seguimiento de la información personal del usuario y la pasa a terceras entidades, generalmente con fines publicitarios**. De hecho, el Spyware se **suele ir acompañado de otro tipo de programas llamados "Adware" (software de anuncios)** que se refiere a una categoría de software que, cuando está instalada en su computadora, puede enviarle pop-up’s

(ventanas emergentes) o anuncios para re-dirigir su Navegador a cierta página Web.

¿Qué efectos provocan en el ordenador?:

1.- Al conectarse a Internet o abrir el navegador **se abren continuamente ventanas emergentes** ('pop-ups').

2.- Cambia la página de inicio y aparecen **nuevas barras de herramientas en el navegador**.

3.- La conexión a Internet, e incluso el **funcionamiento** general de la computadora, **se ralentiza (**el spyware utiliza memoria y ancho de banda).

4.- Si al bajar e instalar un programa de Internet **se instala otra pieza de software** ésta es a menudo 'spyware'.

5.- Aparecen elementos extraños en el ordenador, como **nuevos iconos en el escritorio o botones en la barra de tareas**.

6.- En el navegador aparece un **buscador distinto al habitual**.

¿Qué puedo hacer para evitarlo?:

- Ajuste las preferencias del browser para limitar el uso ventanas pop-up y cookies. Las ventanas pop-up son a menudo generadas por una cierta clase de contenido scripting o activo. Ajustando la configuración dentro de su browser para reducir o restringir el contenido scripting o activo puede reducir el número de ventanas pop-up que aparecen. Algunos browsers ofrecen una opción específica al bloquer o limitar ventanas pop-up. Ciertos tipos de cookies a veces se consideran spyware porque revelan qué páginas del Web ha visitado. Puede ajustar su configuración de privacidad para permitir solamente las galletas del Web site que usted está visitando (véase explorando con seguridad: Contenido y galletas activos para obtener más información).

- No de click en links dentro de ventanas de pop-up - porque las ventanas pop-up son a menudo un producto del spyware, dar click en la ventana puede hacer que instale spyware en su computadora. Para cerrar la ventana pop-up, de click en el icono de "X" en la barra de título en vez de dar click en el botón cerrar o close dentro de la ventana.

- Elija "no" cuando sean hechas preguntas inesperadas - sea cuidadoso de los cuadros de diálogo inesperados que preguntan si usted desea iniciar un programa particular o realizar algún otro tipo de tarea. Seleccione siempre "no" o "cancelar" o cierre el cuadro de diálogo, dando click en el icono de "X" en la barra de título en vez de dar click en el botón cerrar o close dentro de la ventana.

- Sea cuidadoso del software que "Gratis" que descarga - hay muchos sitios que ofrecen barras de herramientas personalizadas o otras características que engañan a los usuarios. No descargue programas de sitios que usted no confía, y dese cuenta que usted puede exponer su computadora al spyware descargando cualquiera de estos programas.

- No siga los links de email que dicen ofrecer software anti-spyware - Estos como los virus de email, pueden servir a un propósito opuesto y realmente instalar spyware el cual ofrece eliminar.

5.- PHISING Y PHARMNG:

5.1.- Phishing:

Viene a significar "pescar, pescando incautos". Es una técnica que se basa en intentar **engañar al usuario** (ingeniería social), normalmente **mediante un correo electrónico, diciéndole que pulse en un determinado enlace, para validar sus claves por tal motivo o tal otro.**

El cuerpo del mensaje es lo de menos, lo importante es que el cliente haga click en el enlace que se le dice, para así **llevarle a una página que él se cree que es de su banco** o caja (porque la han simulado) y así, al poner allí **obtener nuestros códigos** de seguridad.

Si recibís un mensaje de estas características prácticamente seguro que hay gato encerrado, pero si tenéis alguna duda lo más sencillo es llamar por teléfono al banco para solicitar más información, por supuesto, no utilicéis el número de teléfono que viene en el propio mensaje.

De cualquier modo, también hay **métodos para comprobar** rápidamente si la página a la que nos han enlazado es realmente la del banco. Examina las siguientes imágenes que corresponden a **páginas reales de bancos**:

- La url de la página debe comenzar con https://

- En la parte de abajo de nuestro navegador, cuando estamos en un sitio seguro, **suele aparecer un candado**, identificando que el sitio es seguro. Además, haciendo doble-click sobre el candado, se pueden ver las credenciales de seguridad del sitio.

5.2.- Pharming:

El pharming es más peligroso que el phishing, ya que es **más difícil de descubrir**. Se basa en **redirigirnos a la página falsa del banco** diseñada por lo ladrones de forma automática, es decir, **sin que nosotros necesitemos pulsar ningún enlace**. A continuación veremos como lo consiguen, para ello debemos estudiar primero lo que es una dirección IP, un dominio y un servidor DNS:

Cada vez que vosotros ponéis en vuestro navegador, una dirección (por ejemplo www.elmundo.es o www.microsoft.com/spain, ...), **estos nombres que denominamos DOMINIOS** no existen en Internet. En la red, lo que existen son las denominadas DIRECCIONES IP. Por decirlo en lenguaje coloquial: www.cloro.name es nuestro nombre, y la IP asociada sería nuestro número de teléfono.

Una **dirección IP** está formada por **4 números, separados por un punto (.)** y cada uno de ellos puede tener un valor de 0-255 (ver el ejemplo de arriba). Hace una burrada de años se inventó el servicio DNS (Resolución de Nombres) porque es mucho más fácil que los usuarios nos aprendamos una dirección en lenguaje natural que en números.

Si queréis hacer la prueba, en vuestro navegador da igual que escribáis www.elmundo.es o que escribáis http://193.110.128.212 ; vais a ir al mismo sitio. Si ponemos este sitio en letras, alguien tiene que convertirlo a su dirección IP.

¿Quién hace esto?. Pues normalmente nuestro proveedor de servicios, es decir, con el que tenemos contratado el acceso a Internet. Como decíamos nuestro proveedor de servicios dispondrá de un ordenador que funcionará como **Servidor DNS, en cuyo interior hay una base de datos en la que se relacionan los dominios** (www.google.es) **con las ip** (64.233.183.104), puedes imaginar la cantidad de parejas de datos que puede contener dicho servidor, pero ¿Qué ocurre si hay un sitio Web que no se encuentra en dicho servidor?: No pasa nada, el servidor hace una llamada a los servidores DNS que tiene más cercanos hasta que encuentra lo que busca y además de dar respuesta al usuario guarda los nuevos datos, de esa forma, continuamente está aprendiendo.

Ahora bien, ¿Y si alguien accede a estos servidores DNS y modifica los datos que corresponden a tu banco?: La consecuencia puede ser que **cuando intentes acceder a www.cajaduero.es** o www.cajaespana.es r**ealmente lo hagas a la página diseñada por los estafadores**, y cuando teclees tus datos personales para acceder a los servicios ya se habrá culminado el engaño. Por esa razón siempre es importante comprobar que se trata de una página que utiliza el protocolo seguro (https) y que es una página cifrada (el candado), tal como vimos antes.

Pero hay otra forma de realizar dicha estafa, en los sistemas Windows, existe también, desde hace muchos años, una forma de agilizar el trabajo de los servidores DNS, ahorrándole algo de tiempo a nuestro proveedor. Se trata de un **fichero** del sistema llamado **HOSTS**. Cada vez que escribimos una dirección en nuestro navegador, lo primero que hace el sistema es comprobar si esa dirección (ese "host", en términos informáticos) está en el fichero **hosts**, y si es así, nuestro propio ordenador lee la dirección IP que le corresponde y nos enviará allí. Por lo tanto, los estafadores **se pueden meter en nuestro ordenador** para **modificarnos este fichero** a través de un virus o un troyano.

De esta forma, cuando escribamos en nuestro navegador una dirección, estaremos yendo a otra sin saberlo.