

## ❑ Consejos para no sufrir fraudes informáticos [R02]



.....

• Tipos de vulnerabilidades .....	1
• Algunas medidas para protegernos .....	4
• Software básico de seguridad para el puesto de usuario bajo Windows XP/2000/2003 ...	9

.....

Cada vez son más numerosas y complejas las prácticas fraudulentas que ponen en serio peligro la identidad digital de las personas y los bienes a los cuales se puede acceder por esta vía. El phishing, la pérdida de datos, el robo de la señal Wi-Fi, el MalWare y el robo de la propia identidad son riesgos que este trabajo explica como minimizar.

### • Tipos de vulnerabilidades

1. **Phishing:** Se trata de una estafa que se realiza a través del correo electrónico. El estafador o phisher envía lo que parece una comunicación oficial del banco del usuario o cualquier otro organismo de cara a obtener su información privada, como la contraseña para operar a través de Internet con el banco, etc.

Medidas contra el Phishing:

- Nuestro banco o cualquier otra organización nunca nos va a solicitar datos a través de e-mail, ni siquiera por teléfono, por ello nunca rellene ningún formulario de su banco que le llegue a través de e-mail.
- Navegadores de última generación como Firefox 2.x (<http://www.mozilla.org>) e Internet Explorer 7 vienen equipados con herramientas antiphishing. En el caso de Firefox, incluso puede informar acerca de la URL (Universal Resource Locutor) falsa, y el caso quedará registrado en la base de datos de sitios phishing de tal forma que si otro usuario ingresa (usando el mismo navegador Firefox), automáticamente se le avisará que ha ingresado a un sitio Web previamente notificado como falso.

2. **Pérdida de datos:** Perder lo que almacenamos en nuestra computadora puede ser una catástrofe: las fotos de nuestras vacaciones, nuestras películas, nuestra música, etc. Un simple apagón, un virus o un fallo en el disco duro puede mandar al limbo informático todos estos datos.

Medidas contra la Pérdida de Datos:

- Copia de seguridad o backup: es importante que se realice de forma periódica una copia de seguridad. Puede hacerlo de forma manual, guardando la información en medios extraíbles (disco duro, cd-rom grabable, cintas magnéticas, discos ZIP, JAZ o dispositivo de almacenamiento USB) o con programas especialmente creados para realizar copias de seguridad.
  - Existen programas informáticos especializados en rescatar datos perdidos, pero de todas formas no siempre será rescatable el 100% de la información. Así que es mejor prevenir que tener que lamentar, es decir, realice regularmente copias de seguridad de su información.
3. **Robo de señal Wi-Fi:** Muchas veces hemos oído eso de "mi vecino me roba la señal inalámbrica de conexión a Internet".

Medidas para proteger nuestra red inalámbrica:

- Habilitar contraseña de red y de administrador del router inalámbrico, cambiando las que vienen por defecto del fabricante u operador de telefonía (habitualmente "1234", etc.).
  - Filtros MAC: Cuando un equipo informático se conecta a Internet se le asigna una dirección IP. Sin embargo, hay otro tipo de identificador o número distintivo único que no pertenece al PC, ni se configura mediante el Sistema Operativo, sino que está asociado a la tarjeta de red del equipo informático directamente, este identificador se denomina número MAC y es único a nivel mundial para cada una de las tarjetas de red de los distintos fabricantes. Por ello es posible habilitar un filtro en los routers Wi-Fi para que sólo se conecten a nuestra red los dispositivos con un determinado número MAC.
  - Límites DHCP: una forma sencilla de evitar robos de señal es limitar el número de computadoras que pueden conectarse a la misma. Esto es posible a través del servicio DHCP del router, que se encarga de asignar direcciones IP automáticamente a cada equipo informático que se conecta a él. Así, si tenemos dos PC, con direcciones IP correlativas, acotaremos el rango entre los números de estas direcciones y así ningún otro ordenador podrá entrar a nuestra red porque no habrá direcciones IP disponibles. Esto se configura habitualmente en los routers Wi-Fi en la sección DHCP : "Ip Inicial – Ip Final".
4. **Robo de Identidad:** En ocasiones usamos claves para acceso a servicios on-line fácilmente descifrables (la fecha de nuestro cumpleaños, nuestro nombre con algún número sencillo a continuación, o el básico 1234).

Medidas para protegernos contra el robo de identidad:

- Contar con una buena contraseña de construcción compleja. Para ello es importante evitar contraseñas que tengan algún significado, como nuestra fecha de nacimiento, nuestro teléfono, etc. Evitar palabras en cualquier idioma que puedan estar en un diccionario, ya que existen sofisticados programas de

ataques por diccionario que comprueban las coincidencias con todas las palabras de un idioma. Es importante que la contraseña contenga letras mayúsculas, minúsculas y números, siendo deseable que también incluya algún carácter distintos de estos (\*, -, +, etc.)

- Nunca enviar contraseñas por e-mail, Messenger, chats, etc.
- No emplear la misma contraseña para todos los servicios.
- Intente cambiar periódicamente la contraseña.

Una posible técnica para construir una contraseña puede ser recordar una frase que nos diga algo, coger la inicial de cada palabra, poner una letra en Mayúsculas y añadirle algún número significativo para nosotros, ej.

- Frase a recordar: “Mi departamento es el que mejores servicios ofrece”
- Número a recordar : 76
- Una posible contraseña de calidad 7 sobre 10 : “Mdeeqmso76”
- Otra posible contraseña de calidad 9 sobre 10 : “Mdeeqmso(76)”

5. **Malware:** Las formas más comunes de MalWare son los virus, que intentan provocar funcionamientos anómalos en nuestro ordenador, los troyanos que permiten el acceso remoto, y el spyware, adware y bots, que son MalWare (Malicious Software) que recopilan información sobre el dispositivo y la persona que lo utiliza para enviar ésta a posteriori al exterior (empresas de marketing para la elaboración de perfiles comerciales según nuestros hábitos de navegación, etc.).
6. **Entrada no autorizada a nuestro ordenador desde redes de comunicación:** Se estima que hoy en día un ordenador conectado a una red pública de comunicaciones, como Internet, no aguantará más de 15 minutos sin sufrir algún intento de intrusión directa desde la red pública de comunicaciones. Por este motivo, junto a que MS Windows es un sistema que por defecto se instala con múltiples servicios de entrada activos (carpetas compartidas, etc.), es necesario tener en funcionamiento algún tipo de cortafuegos personal siempre en nuestro PC, el cual nos avisará ante cualquier intento de entrada o salida de datos de nuestro ordenador para que autoricemos ésta expresamente.
7. **Explotación de vulnerabilidades de nuestro Sistema Operativo y programas de Internet (navegador Web, etc.):** Los sistemas operativos actuales, y en especial los de la familia de Microsoft, contienen múltiples vulnerabilidades que los intrusos aprovechan para, mediante su explotación, entrar en nuestro PC o enviarnos algún tipo de Malware. Es muy importante, para evitar esto, mantener los sistemas al día con las últimas actualizaciones de seguridad disponibles del fabricante (ej. Actualizaciones Windows :

<http://windowsupdate.microsoft.com>

Nota: En la siguiente dirección encontrará información actualizada sobre nuevas vulnerabilidades del software de MS y noticias de seguridad de interés:

<http://alerta-antivirus.red.es>



- Algunas medidas para protegernos

Además de las medidas indicadas en el apartado anterior, expondremos a continuación algunas medidas adicionales necesarias de aplicar para minimizar el riesgo de sufrir un fraude informático.

- Consejo 1: Un protocolo de seguridad antivirus/MalWare

- Instalar un antivirus de calidad y software anti espía (spyware) y asegurar al menos semanalmente, siendo deseable a diario, la actualización de las bases de datos de virus.
- Chequear CDs antes de acceder a sus contenidos, sólo una vez, al comprarlos o adquirirlos y marcarlos de tal modo que se pueda verificar a posteriori el chequeo. En el caso de CDs regrabables, deberán chequearse cada vez que se acceda a ellos y no tan solo una vez.
- Formatear todo disquete virgen, dispositivo USB, etc., adquirido nuevo, ya que pueden contener virus aún desde el proceso de fabricación.
- Revisar todo disquete o dispositivo externo que provenga del exterior, es decir que no haya estado bajo nuestro control, o que haya sido introducido en el PC.
- Si nos entregan un dispositivo de almacenamiento externo (disquete, USB, etc.) y nos dicen que está revisado, NO CONFIAR NUNCA en los procedimientos de otras personas que no seamos nosotros mismos. Nunca sabemos si esa persona sabe operar correctamente su antivirus. Puede haber revisado sólo un tipo de virus y dejar otros sin controlar durante su escaneo, o no tener actualizado su antivirus.
- Para bajar páginas de Internet, archivos ejecutables, etc., definir siempre en el PC una carpeta o directorio para recibir el material, y escanear con el antivirus. Nunca ejecutar o abrir antes del escaneo ningún tipo de software.
- Evite navegar por sitios Web de dudosa reputación, como sitios warez (sitios que ofrecen programas y cracks, serial, key maker u otros para activación de software).
- Nunca abrir un adjunto de un e-mail sin antes chequearlo con nuestro antivirus. Si el adjunto es de un desconocido que no nos avisó previamente del envío del material, directamente borrarlo sin abrir.
- Al actualizar el antivirus, verificar el PC completamente -análisis completo-. En caso de detectar un virus, proceder a verificar todos nuestros soportes que hayan tenido contacto con el PC (disquetes, CDs, USB, ZIP's, etc.)

Quien navega en Internet nunca estará totalmente exento de ser víctima de algún software maligno o de un ataque informático, pero con los anteriores consejos se puede minimizar la exposición. De su grado de cuidado y precaución dependerá el no ser víctima de este tipo de fraudes.

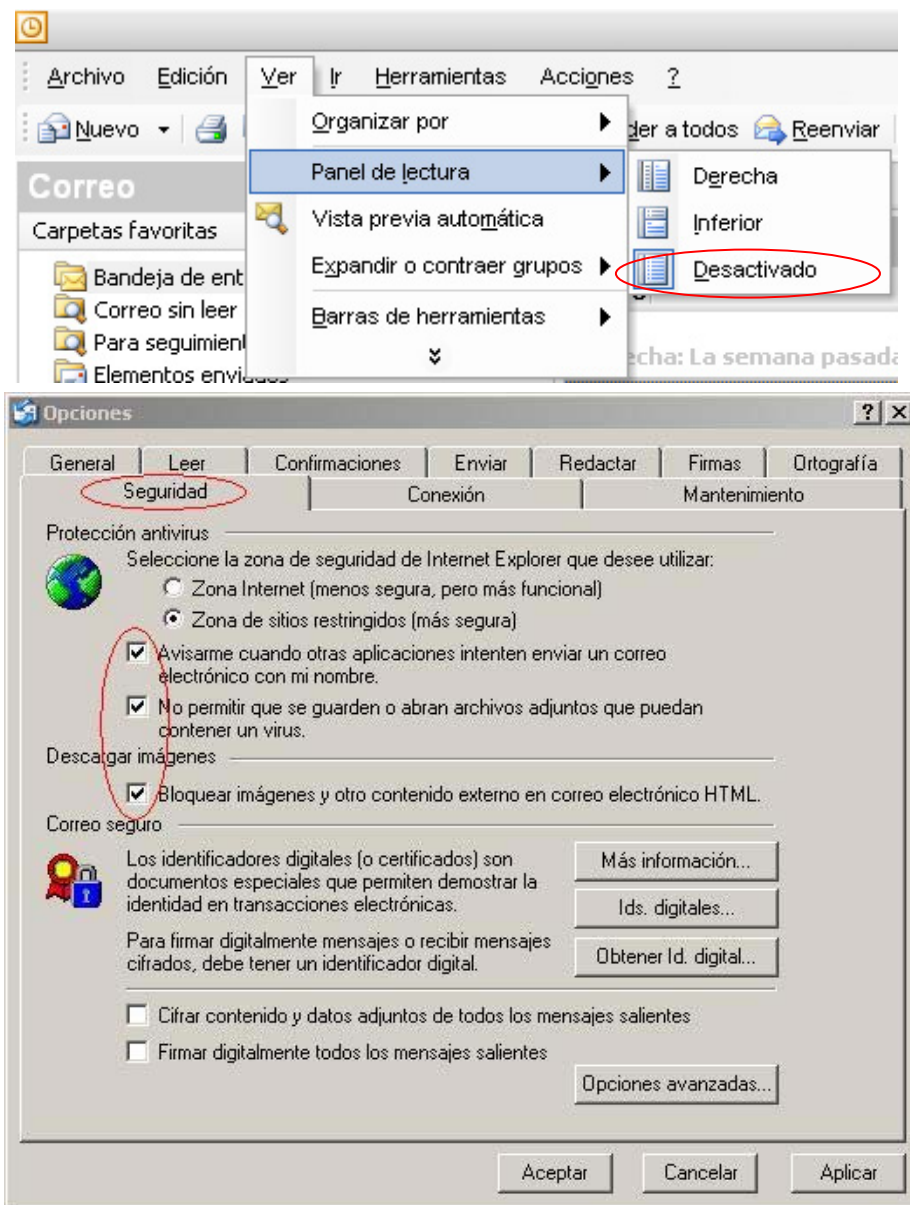


- Consejo 2: Protección en el uso de correo electrónico

- No ejecute ficheros de programa, o cualquier otro tipo de ficheros adjuntos -típicas gracias navideñas, etc.-, que le envíen por correo electrónico, a menos que esté seguro de su origen y contenido. Así evitará virus, troyanos y otro tipo de MalWare en su equipo informático.
- A la hora de confiar en algún fichero adjunto que le hayan enviado por correo electrónico, según el emisor del mismo, tenga en cuenta, que muchos virus y otro tipo de MalWare, una vez ha infectado un equipo informático, pueden reenviarse automáticamente a todas las direcciones de correo de la libreta de direcciones del equipo infectado, simulando ser el propietario del equipo. Por este motivo, incluso en el caso de confiar en el origen de un correo -correo proveniente de un emisor conocido-, desconfíe de éste y sus ficheros adjuntos en aquellos casos en que el Asunto de dicho correo incluya textos en inglés, no habituales de la persona que le envía el correo -emisor-, etc.
- En cualquier caso recuerde, **NO ABRA NUNCA UN FICHERO ADJUNTO EN SU CORREO ELECTRÓNICO SIN ANTES VERIFICAR SU AUTENTICIDAD DE ORIGEN Y CHEQUEAR SU CONTENIDO CON UN ANTIVIRUS ACTUALIZADO.**

Nota. Para escanear un fichero adjunto, guárdelo en una carpeta temporal sin abrir este, y a continuación chequee dicho fichero con su antivirus, tan solo en el caso de que su Antivirus dé el visto el bueno al fichero adjunto tras su escaneo, puede proceder a abrir éste.

- Desactive la visualización automática de los ficheros adjuntos y contenido de correos, en su software de correo electrónico. De este modo evitará otros tipos de ataques que se producen, ya no mediante ficheros adjuntos infectados, sino mediante códigos de ataque introducidos en el propio contenido del correo electrónico -texto del mensaje-.



De este modo, al pinchar sobre la línea de un nuevo correo, este no mostrará su contenido automáticamente, pudiendo usted eliminarlo de forma segura en casos de no reconocer claramente al emisor. Para ver su contenido deberá hacer expresamente "doble clic" sobre el correo.



### • Consejo 3: Como protegerse del phishing

- El phishing es una modalidad de estafa con el objetivo de intentar obtener de un usuario sus datos, claves, cuentas bancarias, números de tarjeta de crédito, identidades, etc. Resumiendo "todos los datos posibles" para luego ser usados de forma fraudulenta.
- Se puede resumir de forma fácil, engañando al posible estafado, "suplantando la imagen de una empresa o entidad pública", de esta manera hacen "creer" a la posible víctima que realmente los datos solicitados proceden del sitio "Oficial" cuando en realidad no lo es.
- El phishing puede producirse de varias formas, desde un simple mensaje a su teléfono móvil, una llamada telefónica, una Web que simula una entidad, una ventana emergente, y la más usada y conocida por los internautas, la recepción de un correo electrónico. Pueden existir más formatos pero en este documento solo mencionamos los más comunes;
- Una primera y eficaz medida de protección, es no hacer clic en enlaces a direcciones Web que le envíen entre el texto de un correo electrónico, dado que la dirección de destino puede estar falseada y usted sufrir un ataque de "PHISING".
- Si tiene que acceder a una dirección Web o enlace contenido entre el texto de un correo electrónico, en lugar de hacer clic directamente sobre el enlace, haga lo siguiente:
  - a. Pulse el botón Derecho del ratón sobre el enlace (botón secundario del ratón, botón derecho y no principal), y elija la opción "Copiar /Copiar dirección de enlace" del menú de opciones que le aparecerá.
  - b. A continuación, abra su navegador Web y pulsando de nuevo el botón Derecho del ratón sobre la zona de la barra superior de direcciones -URL-, elija la opción "Pegar".
  - c. Finalmente, compruebe antes de pulsar la tecla Intro para acceder a la dirección recién pegada en la barra de direcciones de su navegador, si la dirección coincide con exactitud con la del Web al que pretendía acceder.

Ej. [www.cajamadrid.es](http://www.cajamadrid.es) -> Dirección correcta

[www.oicajamadrid.net](http://www.oicajamadrid.net) -> Dirección falseada.

En el siguiente ejemplo, se puede observar como se intenta falsear la dirección de Cajamadrid, si usted en lugar de pinchar directamente en el enlace incluido en el correo electrónico, accede mediante el método descrito, podrá observar claramente la falsificación en la barra de direcciones de su navegador Web, por bien que haya sido falseado una Web para simular ser Cajamadrid e intentar engañarle.



- Recuerde, para visitar sitios Web que le envíen en un correo electrónico, teclee la dirección de cada sitio directamente en la barra de direcciones -URL- de su navegador Web, o pegue esta tras copiarla de su correo electrónico. No acceda NUNCA POR ENLACES PROCEDENTES DE CUALQUIER SITIO, y en especial que le hayan llegado por correo electrónico.
- Finalmente, recuerde que su entidad bancaria o similar, NUNCA le enviará una solicitud de cambio de contraseña, modificación de sus datos bancarios, etc., por correo electrónico.
- Otras medidas genéricas de protección contra el phishing recomendadas por "RED.ES" son:
  - 1.- No atienda a correos electrónico escritos en idiomas que no hable: su entidad financiera no se dirigirá a Ud. en ese idioma si antes no lo han pactado previamente.
  - 2.- No atienda a correos enviados por entidades de las que no es cliente en los que le pidan datos íntimos o que afecten a su seguridad.
  - 3.- No atienda a sorteos u ofertas económicas de forma inmediata e impulsiva.
  - 4.- No atienda a correos que le avisen del cese de actividades financieras recibidos por primera vez y de forma sorpresiva.
  - 5.- No atienda a correos de los que sospeche sin confirmarlos telefónica o personalmente con la entidad firmante.

- Software básico de seguridad para el puesto de usuario bajo Windows XP/2000/2003

- **Antivirus:**

- NOD32. Antivirus comercial de reconocido prestigio y muy ligero: ocupa pocos recursos del ordenador, algo importante ya que no sobrecargará nuestra máquina haciéndola más lenta como ocurre con otros antivirus. Página oficial en español: <http://www.nod32-es.com>
- Kaspersky. Antivirus comercial también de reconocido prestigio y con múltiples galardones. Página oficial en español: <http://kasperskytienda.com.es/>
- AVG. Antivirus libre de coste, a pesar de lo cual supera en nivel de detección a muchos otros antivirus comerciales. Página oficial de descarga: <http://free.grisoft.com/doc/5390/Ing/us/tpl/v5#avg-anti-virus-free> (Download Now).

- **Navegador Web:** Alternativa a Internet Explorer con mayores niveles de seguridad y actualizaciones automáticas transparentes al usuario: "Mozilla FIREFOX". Página oficial: <http://www.mozilla-europe.org/es/products/firefox/>

- **Firewall.** Windows XP incorpora un cortafuegos básico por defecto, asegúrese que está activo en "*Inicio>Panel de control>Firewall de Windows*", o en su defecto utilice alguno de los cortafuegos personales disponibles en el mercado, como puede ser "Outpost", producto comercial pero del cual existe una versión básica libre de coste. Descarga Outpost<sup>1</sup> libre de coste:

<http://www.agnitum.com/products/outpostfree/download.php>

En esta dirección puede obtener una copia de la versión comercial válida durante 30 días (Outpost-PRO), tras lo cual deberá adquirir una licencia de usuario final:

<http://www.outpost-es.com/home/index.html>

En esta otra dirección encontrará un manual en castellano del uso de este avanzado firewall personal :

[http://www.outpost-es.com/support\\_guia\\_rapida\\_online/index.html](http://www.outpost-es.com/support_guia_rapida_online/index.html)

---

<sup>1</sup> Nota: El programa Outpost, en su versión libre de coste, puede preguntar durante los primeros días si desea conceder acceso a Internet a distintas aplicaciones que usa habitualmente, entre ellas el propio "Outpost", en caso de que deje que dicha aplicación (Outpost) acceda a Internet, éste bajará la versión comercial del producto y la instalará en su equipo eliminando la versión libre de coste que ud. ha instalado, con lo que a los 30 días dejará de funcionar salvo que ud. adquiera una licencia comercial del producto, si no desea que ocurra esto y quiere seguir utilizando la versión libre de coste indefinidamente, no permita a Outpost acceder a Internet.



- **Anti Spyware:** Las herramientas de este tipo eliminarán los distintos tipos de software espía que muchas páginas de Internet por la simple navegación en sus contenidos instalarán en nuestro PC.
  - Ad-Aware. Es el producto anti-spyware más popular de toda la red, muy efectivo y con actualizaciones disponibles prácticamente a diario. Es una **herramienta pasiva** para chequear, que deberemos pasar a nuestro ordenador al menos semanalmente, o a diario si navegamos por sitios potencialmente peligrosos (contenidos eróticos, etc.). A pesar de ser comercial tiene una versión para usuarios personales (no empresa) libre de coste. Descarga versión libre de coste:

[http://www.lavasoftusa.com/products/ad-aware\\_se\\_personal.php](http://www.lavasoftusa.com/products/ad-aware_se_personal.php).

En el Anexo. A de este documento se incluye un pequeño manual del uso de esta herramienta.

- Spyware. Blaster. Previene la instalación automática de spyware, MalWare, activeX, dialers, hijackers, y otro tipo de software espía potencialmente peligroso. Igualmente bloquea la entrada de cookies rastreadoras, etc. Puede parecer algo complicado de utilizar, pero tras instalarlo no tenemos que preocuparnos de pasarlo periódicamente a nuestro PC, ni siquiera ejecutarlo, pues estará siempre arrancado y trabajando en segundo plano al igual que nuestro antivirus. Este software está igualmente libre de coste.

Página oficial: <http://www.javacoolsoftware.com/spywareblaster.html>

Las dos herramientas presentadas: Ad-Aware y Spyware Blaster son totalmente compatibles entre sí, pudiendo tener instaladas ambas sin ningún tipo de incompatibilidad entre ellas, y siendo esto recomendable para tener una de ellas en segundo plano trabajando continuamente (Spyware Blaster) y la otra (Ad-Aware) con una ejecución manual de rastreo por ej. Semanal para que elimine lo que no haya detenido la anterior.<sup>2</sup>

---

<sup>2</sup> Nota: Como hemos visto, dos buenos compañeros de viaje para la seguridad de nuestro equipo informático son el firewall personal OUTPOST y el antivirus NOD-32, en la siguiente dirección existen oferta especiales de la venta conjunta de ambos productos. :

[http://www.outpost-es.com/purchase/purchase\\_oe.html](http://www.outpost-es.com/purchase/purchase_oe.html)

- Anexo A. Manual Ad-Aware.

Ad-Aware SE Personal Build 1.06 es una poderosa herramienta que se usa para detectar objetos ofensivos instalados sin autorización en nuestro PC por la simple navegación en ciertas páginas Web (spywares, awares, etc).

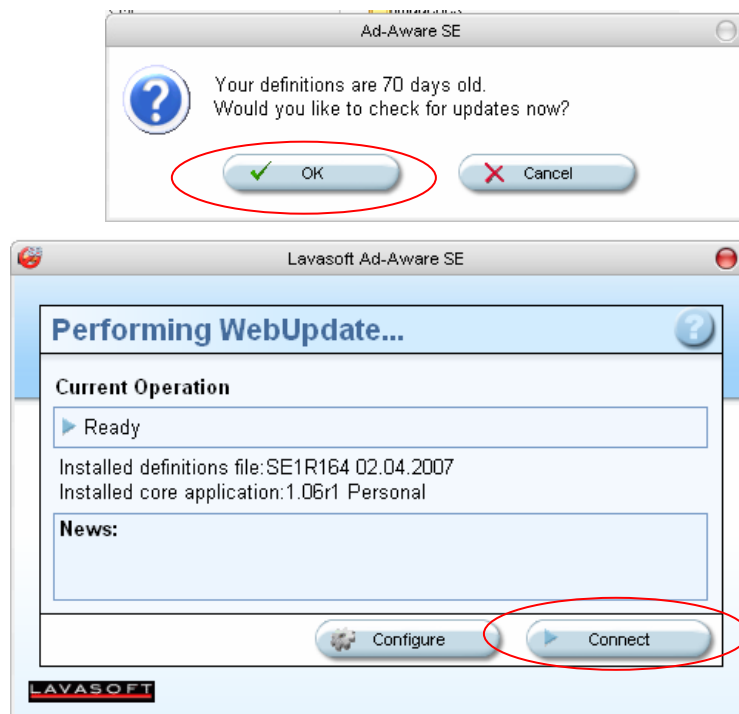
Este software actualiza su base de datos periódicamente, siendo esto muy importante a la hora de luchar contra estos parásitos y dándole al usuario la posibilidad de ponerlos en cuarentena y eliminarlos sin perjuicios de su equipo informático

Para instalar el software descargue este previamente de la URL:

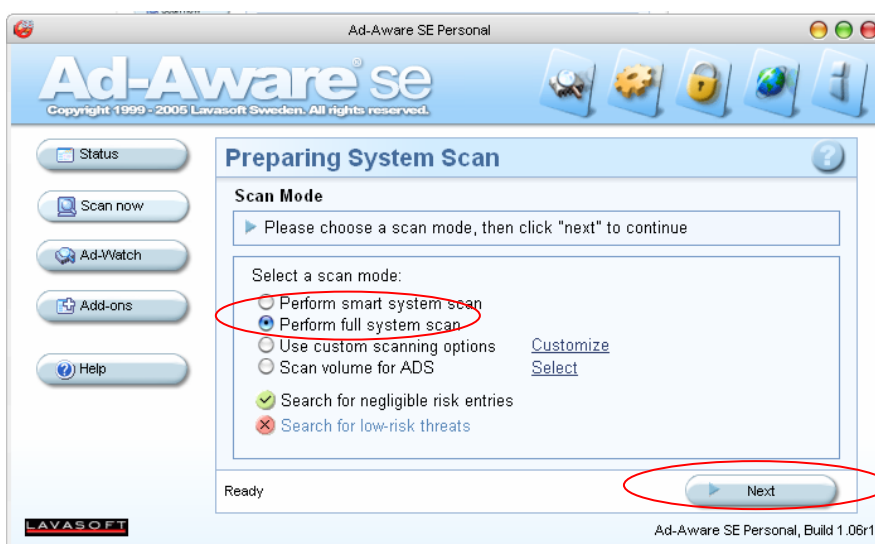
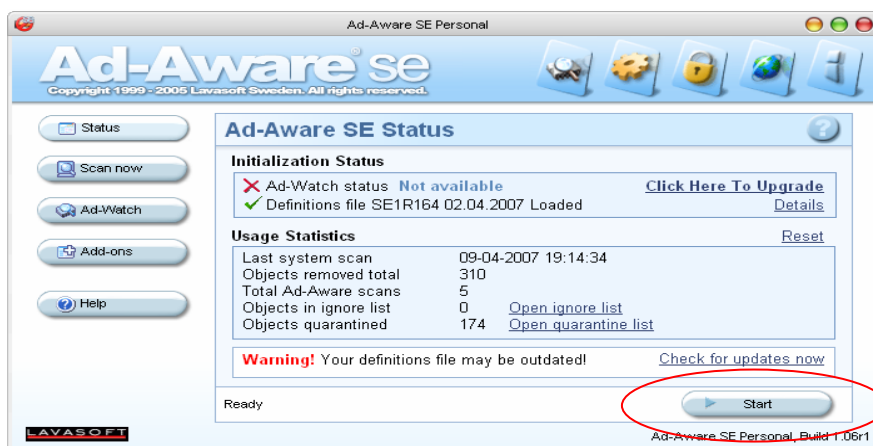
[http://www.lavasoftusa.com/products/ad-aware\\_se\\_personal.php](http://www.lavasoftusa.com/products/ad-aware_se_personal.php).

Obtendrá un único archivo ejecutable denominado "**aawsepersonal.exe**", haga doble clic sobre éste y comience la instalación, pulsando simplemente "*Siguiente /Next*" en las distintas ventanas de instalación que aparecerán.

Una vez instalado, al ejecutarlo por primera vez, nos mostrará la pantalla principal en la cual es recomendable, como primera medida, buscar la última actualización disponible para tener su base de datos de software espía actualizada. Para eso hacemos clic en "*Check for updates now (Buscar actualización ahora)*" y el botón "*Connect*" para que Ad-Aware SE se conecte con el servidor de Lavasoft y busque la más reciente actualización.

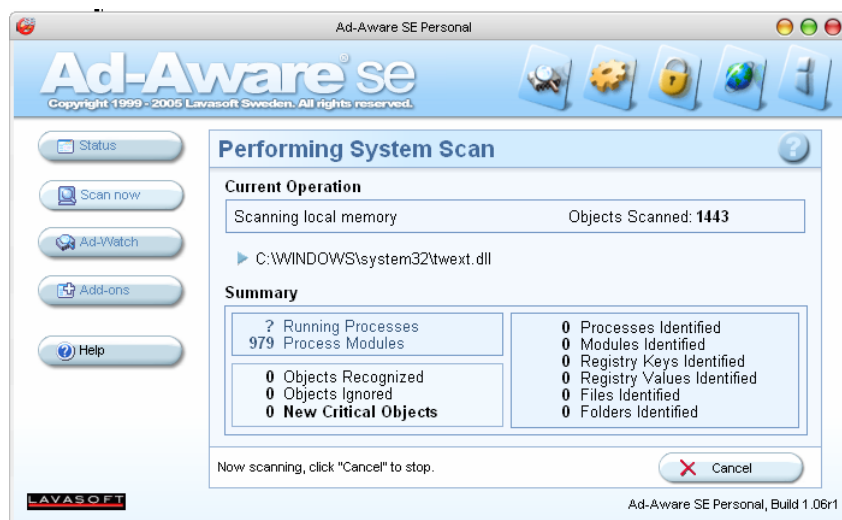


Una vez actualizado y tras arrancar el programa, en la pantalla principal apretar el botón de "Start" donde aparecerá el Modulo de Análisis en el que elegiremos en que modo escanear el PC.

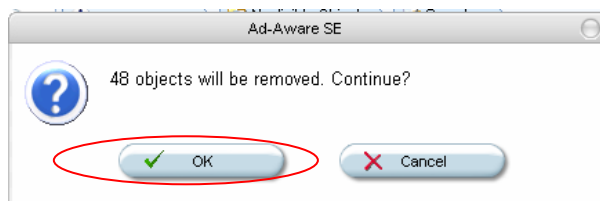
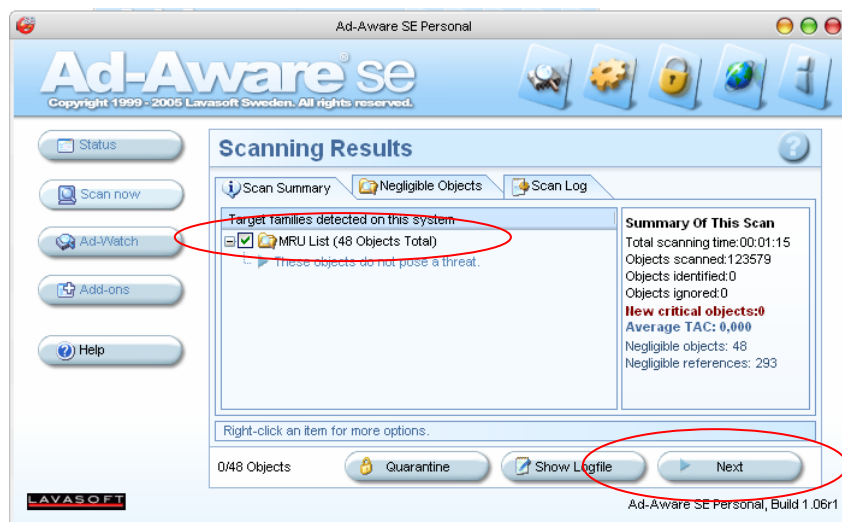


- Perform smart system scan (Realizar exploración del sistema optimizada): Ésta es la opción que viene por defecto, la cual realiza un análisis rápido del sistema.
- **Perform full system scan** (Realizar exploración completa del sistema): Es la opción más recomendable para analizar nuestro sistema la primera vez que ponemos en marcha el Ad-Aware SE para buscar a fondo estos parásitos (spyware).
- Use custom scanning options (Usar opciones personalizadas): Esta opción permite seleccionar que archivos, carpetas, o unidades de disco queremos analizar.
- Scan volume for ADS (Volumen de exploración para ADS): Esta opción busca ADS (Cadenas de Datos Alternativas). Realiza su funcionamiento en dos partes. Primero analiza el sistema y guarda la información de cada archivo individualmente y después analiza en detalle toda la información relacionada con cadenas de datos. Esta opción requiere que el usuario seleccione carpetas o unidades para llevar a cabo el análisis.

Una vez elegida la opción de análisis presionamos el botón "Next" como se muestra en la figura anterior, tras lo cual el programa examinará en detalle nuestro PC, como se puede observar en la siguiente figura:



Una vez finalizada el análisis de nuestro sistema nos indicara los resultados en una pantalla similar a la que se muestra a continuación, en la que tenemos la opción "Show Logfile" (que mostrara información detallada de los spywares encontrados) y la opción de "Next", que mostrará la siguiente pantalla de selección de lo que se va a eliminar, siendo recomendado seleccionar todos los objetos encontrado marcando su casilla correspondiente, y pulsar de nuevo el botón "Next" para la eliminación.



Tras esto, podremos cerrar el programa, no olvidando ejecutar éste de nuevo con periodicidad al menos semanal.