

Riesgo Informático – "Spyware", "Adware" y "Popup"

Preparado por Ing. Simón Mario Tenzer, Octubre 2004 ¹

Material exclusivamente con fines docentes, tomado de Microsoft, Jerry Honeycutt, 20 de Abril de 2004, y otras fuentes.

Como si no fuésemos suficientes con los "spam"², los virus³ y los gusanos⁴ ahora han llegado el "Adware" y "Spyware" para acabar con lo poco que queda de productividad y privacidad. Las "cookies"⁵ son completamente inofensivas en comparación!

Adware es el software que muestra publicidad en la computadora. Se trata de anuncios que aparecen de repente en pantalla incluso aunque no se esté navegando por Internet. Algunas empresas ofrecen software "gratuito" a cambio de publicidad que aparece en pantalla. Así es como hacen dinero.

Spyware es un tipo de software que manda información personal, de uno mismo, registrada en la computadora a terceros sin dar el consentimiento o sin saberlo. Este tipo de información puede ir desde los sitios Web que han sido visitados hasta más delicados como nombre de usuario y contraseña⁶. Por lo general, las empresas con pocos escrúpulos utilizan esta información para enviar publicidad no solicitada.

Hay quienes piensan que Windows XP, Windows Media Player y Windows Messenger es spyware. La razón por la que supuestamente no lo sería, es que Microsoft ofrece una "combinación importante de avisos de privacidad" y deja a los usuarios la decisión sobre la utilización de los servicios Web o sobre compartir la información. Por ejemplo, la primera vez que ejecuta Windows Media Player 9 Series, el usuario tiene la oportunidad de revisar las opciones de privacidad e ir haciendo cambios para que se adapten a él.

¿Su computadora se ha visto afectado por Spyware?

El principal problema de estos programas es que interfieren en los resultados de la computadora. Por ejemplo, Internet Explorer puede pasar a funcionar mal, puede colgarse la computadora con más frecuencia o reducir su velocidad de ejecución. Lo difícil que es eliminar con éxito el spyware hace de la prevención la prioridad indiscutible.

Por lo general el "adware" y el "spyware" se instalan sin permiso en su equipo siguiendo uno de estos métodos:

- Engañándole para que haga clic en el enlace que lo instala⁷. Los enlaces a spyware no lo parecen. Por ejemplo, un sitio Web que está intentado poner spyware en su computadora

¹ Con la colaboración de Cra. Beatriz Pereyra y demás integrantes de la Cátedra Introducción a la Computación.

² Ver textos "Ética e Informática", Comentarios previos y "Riesgo Informático- Nueva modalidad a través de Internet. 'Phishing'", en partes varias.

³ Ver textos "Virus Informático" e "Introducción a Riesgo Informático"

⁴ Ver texto "Virus Informático", gusanos (Works)

⁵ Ver texto "Virus Informático", Lo que no son virus: accesos a Internet.

⁶ Ver texto "Riesgo Informático- Nueva modalidad a través de Internet. 'Phishing'".

⁷ Ver texto "Internet, una herramienta para los negocios." de Beatriz Pereyra, Ataques a las contraseñas con técnicas de ingeniería social

puede abrir una ventana que parece un cuadro de diálogo de Windows y engañarle instalándolo cuando pulsa el botón Cancelar del cuadro de diálogo. A veces, los que promocionan spyware pondrán un título de mentira en la barra en una ventana vacía y luego instalarán spyware cuando intenta cerrar la ventana.

- ❑ Al instalar software gratuito en el que está incluido. Por ejemplo, puede instalar un programa de archivo compartido que le instala spyware sin que usted lo sepa. Los programas en los que se comparten los archivos pueden ser una gran fuente de adware.

Una vez que se ha instalado el spyware puede transmitir su información personal y descargar publicidad durante las 24 horas del día en su computadora. Del mismo modo se puede hacer con la configuración de su buscador, como por ejemplo, su página de inicio y la página de búsqueda.

Cómo protegerse ante Spyware y Adware

Si no cuenta con ayuda no tiene ninguna posibilidad de evitar que el "adware" o el "spyware" entre en su equipo. Los antiguos programas de antivirus ni siquiera pueden evitar el adware, ya que no los consideran ni virus ni gusanos. En primer lugar, por lo general el usuario da permiso para la instalación del adware en su computadora aunque lo hace de una forma inconsciente porque los enlaces con los que se transmiten son bastante engañosos. En segundo lugar, el adware no se comporta como un virus o un gusano normal. De hecho no hacen un daño real, aparte de arruinar su funcionamiento, y no utilizan su agenda de direcciones para propagarse (aunque algunos tipos de adware pueden estropear sus herramientas de spyware).

Algunos productos de software antivirus incluyen herramientas para buscar adware y spyware. Por ejemplo, las últimas versiones de McAfee VirusScan, Norton AntiVirus 2004 y Trend Micro PC-Cillin 2004 analizan los equipos en busca de adware y spyware.

Cómo evitar que le instalen programas sin su consentimiento

Las empresas que están promoviendo adware y spyware dependen de dos cosas: el deseo del usuario de acceder a software gratuito y su credulidad. Para evitarlo:

- ❑ Asegúrese de que los programas que instala no contiene adware. Muchos de los programas de software gratuito incluyen adware. Así es como ganan dinero los creadores. Si tiene dudas, lea el contrato de licencia con cuidado (por lo general aparecen directamente o a través de un proceso de instalación). Además debería comprobar quién es el creador del sitio Web de donde proviene. Si sigue sin estar seguro, haga una búsqueda en los grupos de Google con el nombre del programa y la palabra clave adware o spyware. Si no encuentra ningún comentario al respecto, entonces es probable que no haya problemas.
- ❑ Instale una herramienta para bloquear los "pop-up" y evitar así las ventanas de adware y spyware. La mayoría del spyware se instala después de haber hecho clic sobre una ventana pop up del buscador. Instale una herramienta para bloquear pop-up y ni siquiera le aparecerá la posibilidad de hacer clic sobre estos enlaces. Dos soluciones gratis son la barra de herramientas de Google y la nueva barra de herramientas de MSN. Las ventanas pop-up además son bastante molestas y hacen perder mucho tiempo. Si es usuario de Windows XP, busque el Service Pack 2 que incluye una serie de características de seguridad, además de una herramienta para bloquear pop-up para Internet Explorer.
- ❑ No instale de manera inconsciente adware o software. Si hace clic sobre un enlace que a primera vista parece inofensivo, y luego aparece un cuadro de diálogo parecido al que hay en la imagen que están en "Ejemplo de un adware" en la hoja siguiente, no haga clic sobre el botón Sí para instalar el software. Si tiene alguna duda no lo haga. Ese cuadro de diálogo es

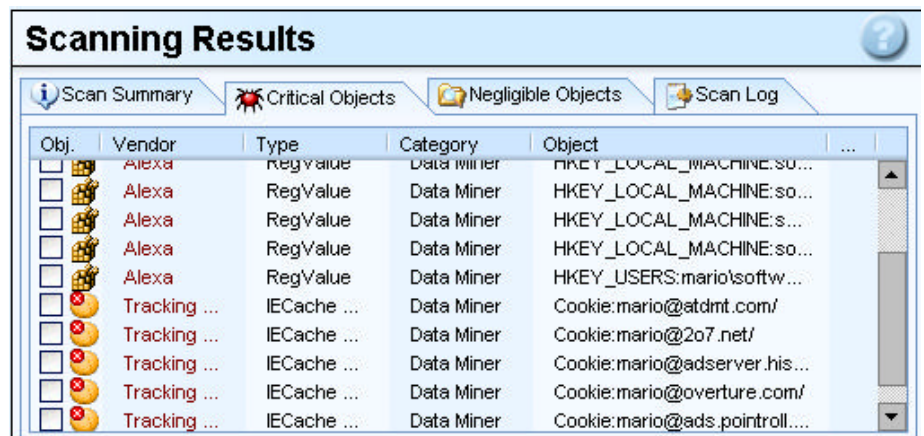
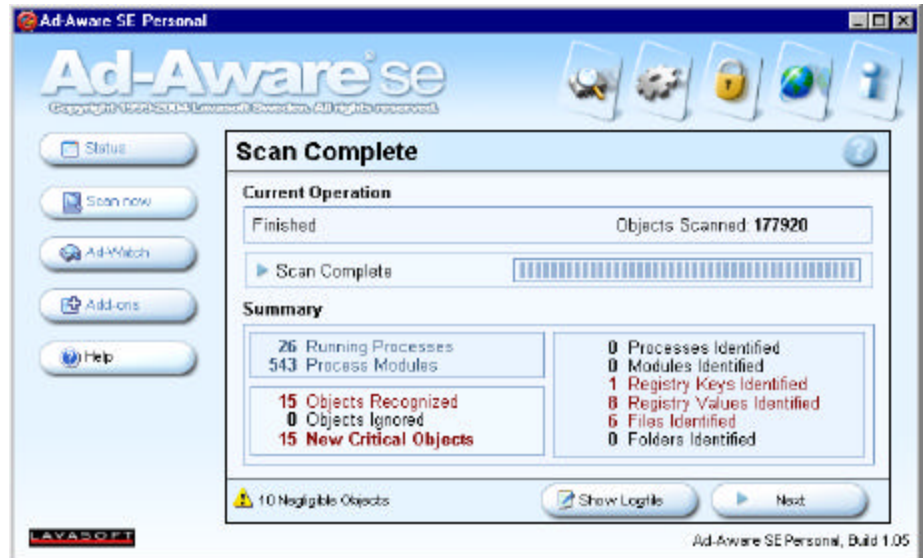
la última línea de defensa de la que depende, y sólo debería instalar de Internet los programas que realmente quiera instalar.

Los buscadores de Spyware y algunos buscadores de virus con firmas de spyware pueden ayudar en la lucha contra el spyware. Sin embargo, la mejor estrategia es tener mucho cuidado con lo que decide descargar e instalar en su equipo.

Revise su equipo

Si está considerando revisar su equipo (computadora) en busca de adware y spyware, entonces es probablemente porque ya esté sufriendo algunos de los síntomas que hemos expuesto anteriormente, como por ejemplo: inestabilidad, problemas de ejecución o control del buscador Web.

Hay software creado para detectar spyware y adware, y para ayudarle eliminarlo. Uno de ellos es "Ad-aware" de Lavasoft. Una versión gratuita está disponible para la utilización particular. También hay disponible una versión comercial para entornos empresariales. Programas como Ad-aware encuentra el adware o spyware que hay en su computadora y luego lo borra.



También puede encontrar herramientas de eliminación de adware y spyware en la guía de "Spyware Protection and Removal": <http://www.firewallguide.com/spyware.htm>. En esta página Web se incluyen enlaces a los programas de eliminación de spyware más conocidos además de una serie de artículos de gran utilidad. Sin embargo si no va a utilizar un programa tan conocido como Ad-aware, busque en los grupos de noticias de Google el programa que ha decidido utilizar. Algunos de los software de eliminación de spyware pueden causar tantos problemas como soluciones y le conviene enterarse de esos problemas antes de proceder a utilizarlo.



Ejemplo de un adware

A modo de ejemplo, se presenta la ventana que sigue. En este caso, avisa explícitamente que incluye cambios y que aparecerán ventanas emergentes. Explica que justamente con estos



servicios es que financia la provisión de soluciones gratis. Es obvio que todos los productos de utilidad que se ofrecen gratis para ser descargados de Internet, de alguna manera es necesario cubrir los costos de desarrollo, de prueba, documentación, soporte de actualizaciones, mantener la página web activa, etc. En estos casos el pago consiste en "comerse" la propaganda no solicitada o en proveer información sobre las actividades que uno realiza (qué páginas consulta, cuándo, etc.)

La mayoría de los adware y spyware se instalan en forma engañosa como se explicó antes.

Programas freeware⁸ y shareware⁹ para detectar y eliminar spyware

SpyBot Search & Destroy 1.3.2b

Tamaño: 4.4 Mb Bajados: 8319
Lic: Freeware Idioma: Español
Windows: 95/98/NT/2000/ME/XP

<http://www.spybot.info/es/index.html>

SpyBot Search & Destroy analiza su disco rígido en busca de Spyware; pequeños módulos que son responsables de las publicidades que muestran muchos programas. Pero muchos de estos programas también transmiten información sobre las páginas que son visitadas, y también otra información más personal. Si SpyBot Search & Destroy encuentra alguno de estos programas puede eliminarlo o reemplazarlo con archivos vacíos (esto es en caso de que el programa host dejara de funcionar sin esos archivos)¹⁰. En la mayoría de los casos, los programas siguen funcionando aún removiendo esos archivos. Soporta Internet Explorer, Netscape Communicator y Opera.

Super Ad Blocker 1.0.1590

Tamaño: 3.8 Mb Bajados: 157
Lic: Shareware Idioma: Inglés
Windows: 95/98/NT/2000/ME/XP

<http://www.superadblocker.com/>

Super Ad Blocker puede bloquear prácticamente cualquier tipo de publicidad que se utilice en Internet: ventanas pop-up, ventanas Flash, pop-under, publicidad en Messenger, publicidad de spyware etc. El programa se actualiza automáticamente a través de Internet, de forma que sus bases de datos siempre están al día. Permite además administrar una "lista blanca" de

páginas web admitidas que no pasarán por el filtro antispam, así como servidores seguros. Se puede deshabilitar momentáneamente usando la tecla CTRL, o cargar los banners bloqueados haciendo click sobre ellos. Dispone de diversas utilidades para borrar los rastros que habitualmente quedan en la PC tras una sesión de navegación por Internet y gestionar cookies, además de unas completas estadísticas y gráficas sobre los anuncios bloqueados.

¿Qué es un pop up? ¿Qué es un pop up killer?

Fuente: http://www.sitiosargentina.com.ar/webmaster/cursos%20y%20tutoriales/programas_pop_killer.htm

Una de las plagas que más irrita a los internautas es la aparición de ventanas emergentes (popup windows) no solicitadas, principalmente con fines publicitarios, cuando se navega por Internet. Su ubicuidad es tal que la mayoría de los internautas habituados han desarrollado unos buenos reflejos para cerrar estas ventanas.

En general, las ventanas emergentes no deseadas se caracterizan por dos razones:

1. Se abre una ventana sin que el usuario lo solicite.
2. Normalmente no contienen controles de navegación, su tamaño es reducido y su intención es publicitaria.

En ocasiones son una pequeña molestia, basta con cerrarlas y no aparecen más mientras se navega en un sitio. A veces son un poco más pesados y aparecen cada vez que cambiamos de página. Y en ocasiones se aterriza en un sitio web diseñado con pocos escrúpulos, que abren una

⁸ Ver textos "Aspectos legales, derechos de autor y piratería de software": Programas shareware, Programas freeware y "Software", Sistema Operativo LINUX

⁹ Ver texto "Internet, una herramienta para los negocios.", Ataque a las contraseñas con Software por la fuerza bruta.

¹⁰ Un ejemplo son algunos optimizadores de descarga de archivos, que son programas de uso gratuito que NO funcionan si se eliminan los adware que tiene asociados. Por ejemplo, DAP presenta publicidad en la ventana de descarga (que NO es spyware), pero, además, tiene rutinas que sí son spyware.

ventana tras otra y se encadena con otros, y se llega a llenar el escritorio de ventanas hasta agotar la memoria del PC y enlentecerlo dramáticamente.

¿Por qué se usan estas ventanas emergentes? Tras descubrir que los anuncios publicitarios incrustados en sus páginas web no funcionaban tan bien como habían previsto, muchas empresas de Internet necesitando paliar un poco las grandes deudas que acarrea ofrecer un servicio gratuito eligieron poner popups en sus páginas de entrada.

¿Cómo se pueden evitar? Existen multitud de programas que anulan la aparición de estas molestas ventanas, llamados "Mata Emergentes" (Popup Killers), tanto gratuitos como pagos.

Para parar las ventanas emergentes hay dos estrategias básicas:

No ejecutar el código que las abre. Suelen ser extensiones del navegador que interceptan las llamadas para abrir nuevas ventanas -en JavaScript es el método `window.open()`- sin que el usuario haya hecho clic en un enlace de la página. En principio son más eficaces puesto que la ventana emergente no se llega a abrir, pero pueden fallar si se abre con otros métodos, como desde una película de Flash.

Reconocer la ventana emergente y cerrala. Suelen ser aplicaciones independientes del navegador que reconocen la ventana por su título, su tamaño, la URL que cargan u otros parámetros y la cierran. Son menos eficientes pero más fiables puesto que no dependen del mecanismo de apertura de la ventana. No obstante pueden fallar si hubiera dos ventanas con las mismas características pero con contenido distinto. Por defecto no bloquean ninguna ventana, ya que hay que indicar expresamente qué ventanas debe cerrar.

Programas pop killer para descargar

A continuación encontrará enlaces a sitios web de programas "Mata Emergentes" gratuitos en español

AdKiller Daemon define una lista con 411 sitios predeterminados, siendo ésta ampliable y configurable. Dispone de una opción que cerrará todas las ventanas que sean menores a un determinado tamaño en píxeles (x,y) definido por el usuario. Guarda en un fichero de registro las ventanas que cierra. Incluye función "Pánico" (cierra todas las ventanas del navegador pulsando Ctrl + p). Instalación: archivo .zip. Una vez descomprimido se ejecuta el fichero `setup.exe`. Se elige el directorio de instalación.

La barra de herramientas de Google incluye un bloqueador de ventanas emergentes, entre otras funciones. Cuando detecta un anuncio entrante, el cursor cambia por un instante. Junto al icono de la barra de herramientas de Google aparece un recuento de la cantidad de ventanas que han sido bloqueadas. Puede indicar al bloqueador de popups que recuerde sitios que transmiten información útil a través de ventanas emergentes. Esta información se guarda en su equipo en una "lista blanca". Instalación: ejecutar el fichero `GoogleToolbarInstaller.exe`. Se acepta el acuerdo de términos y condiciones. Finalmente se elige la configuración y el idioma.

Nopopups inicialmente posee una lista de setenta popups que el usuario irá incrementando manualmente escribiendo en el archivo `nopop.txt` los títulos de los popups que desea que no vuelvan a aparecer. Alternativamente el programa buscará automáticamente la existencia de popups por el título de los mismos. Instalación: archivo .zip. Una vez descomprimido se ejecuta el fichero `nopop.exe`. Se elige el directorio de instalación.

Web Window Killer El programa va creando una "lista hostil" con todos los popups eliminados. Cada vez que aparece un popup no reconocido por Web Window Killer, se añadirá a lista hostil pulsando Ctrl+Shift+k; o también, introduciendo el título del popup manualmente. Dispone de una amplia ayuda en inglés. Almacena un archivo histórico con los popups eliminados. Instalación: ejecutar el archivo "bajado" y a continuación, elegir idioma, aceptar la licencia y por último seleccionar el directorio de instalación.

Mozilla es un navegador completo con numerosas funcionalidades, entre ellas el control de ventanas emergentes. Puede descargar la versión en español desde las páginas del proyecto NAVE: <http://mozilla.metropoliglobal.com/> Puede acceder a esta característica seleccionando el menú Editar, opción Preferencias; bajo la categoría Privacidad y Seguridad aparecen Ventanas emergentes. Ofrece la posibilidad de autorizar ventanas emergentes de sitios Web que especifiquemos. Cada vez que un popup es bloqueado, el navegador lo indica mediante un sonido elegido previamente. Instalación: detalles no relevantes.

Opera es un navegador que incluye la opción de deshabilitar popups. Pulsando la combinación de teclas Alt + P, se visualiza la ventana de Opciones de Opera. Seleccionar el menú Decorado y seguidamente, el submenú Ventanas. Alternativamente, pulsando F12 se despliega un menú emergente donde también se puede decidir habilitar o no los popups. Opera puede admitir ventanas emergentes de sitios Web que se le indiquen. Instalación: detalles no relevantes

La barra de herramientas de Altavista incluye, entre otras utilidades, un bloqueador de popups. Ésta se sitúa por defecto debajo de la barra de direcciones del navegador, igual que la posición de la barra de herramientas Google. Cuando la barra detecta un popup emite un sonido e incrementa un contador. El bloqueo de ventanas emergentes está activado por defecto, aunque puede desactivarlo pinchando en el contador. La barra de herramientas de Altavista se actualiza automáticamente una vez instalada. Instalación: tres pasos; seleccionar idioma, aceptar Contrato de Licencia del usuario de la barra de herramientas, y finalmente se instala automáticamente.

La amplia lista de programas en español, de uso gratuito, para eliminar las ventanas emergentes, se presentó para mostrar que hay diversidad de productos, que trabajan de diferente manera. Cada usuario elige el que mejor se ajusta a su entorno operativo.

Es evidente que al usar una computadora, además del sistema operativo, se necesita tener cargados una serie de programas adicionales, que hoy por hoy son imprescindibles: antivirus, firewall¹¹ (para protegerse de accesos no deseados de terceros), anti adware y anti spyware. Es común tener protector de pantalla dinámico y otras "funcionalidades", que responden al fenómeno del "fatware"¹², haciendo necesario cada vez tener computadoras más potentes.

Algunos de estos productos pueden causar conflicto con los programas de aplicación específicos que se empleen en las organizaciones.

Por último, el sentido común es el recurso más importante al utilizar una computadora y detectar a tiempo los síntomas de presencia de programas maliciosos, como ser funcionamiento lento de la computadora sin explicación razonable, excesivo acceso al disco duro, o cambios ocurridos en el entorno operativo sin haberlos solicitado.

¹¹ Ver textos "Virus Informático": Lo que no son virus: accesos a Internet, "Redes" de S. M. Tenzer: Aprovechamiento de recursos lógicos genéricos, "Intranet": Firewall, "Introducción a Riesgo Informático": Ejemplo de matriz de riesgos.

¹² Ver texto "Software": Tendencias y futuro.

Spyware según un reciente artículo de El Observador (Agencia EFE) (adaptado)

Los "espías" informáticos podrían pagar caro el spyware con la nueva ley en EEUU que propone hasta cinco años de cárcel para los creadores del software que se instala sin permiso del usuario para registrar sus movimientos. Hasta ahora, los creadores de estos programas informáticos han estado a sus anchas por la red, a pesar de las molestias que acarrear.

Microsoft estima que el "spyware" es responsable de la mitad de los fallos que registran los ordenadores personales y de gastos multimillonarios que ocasiona a los fabricantes de ordenadores, proveedores de acceso a la red y personal técnico.

El "spyware" consiste en pequeños programas informáticos -en su mayor parte muy difíciles de detectar incluso por usuarios avezados- que se instalan en el ordenador sin avisar al usuario, como si de un virus se tratase.

La finalidad de estos programas es registrar los hábitos del internauta (por ejemplo, con respecto a páginas visitadas y tiempo que pasa en cada una de ellas), una valiosa información que luego puede usarse para marear al consumidor con anuncios de publicidad a la medida.

La legislación en marcha en EEUU se dirige también a los ataques de "phishing"¹³ (o "pesca" en el argot informático) esto es, los correos electrónicos que emplean argucias para hacerse con información financiera como números de tarjetas de crédito.

Estos modernos timadores habitualmente utilizan los logotipos de compañías como el banco Citigroup o remates por Internet de eBay para hacerse con estos datos.

Otra propuesta de legislación prevé una serie de directrices que obligatoriamente deberán cumplir las compañías de software, como la de solicitar el permiso explícito de los consumidores para instalar algunos programas con los que puedan tener acceso a sus datos.

Quienes violen las nuevas normas se enfrentarían a multas que pueden alcanzar millones de dólares.

Por otra parte, recientemente, en octubre de 2004, la Comisión Federal de Comercio de EEUU (FCC, por sus siglas en inglés) interpuso la primera demanda contra una empresa de Nuevo Hampshire acusada de infectar los ordenadores con software no solicitado para tratar después de vender el remedio para limpiarlos: un programa llamado "Spy Wiper" que cuesta 30 dólares. El acusado es Stanford Wallace, llamado el "rey del spam"¹⁴. El programa también tiene otros nombres, como ser: Spy Deleter, Spydeleter y Spywiper¹⁵

La actuación de la FCC arremete contra una modalidad muy extendida: los programas que prometen limpiar el ordenador de "spyware" pero que no son sino una herramienta de espionaje más.

Esto supone que muchas veces es peor el remedio que la enfermedad, ya que los programas son "agentes dobles": eliminan el software de la competencia para instalar el propio.

Sea como fuere, acabar con esta plaga no resultará fácil, ya que se trata de un software que suele ser más complejo que los virus informáticos y además se renueva constantemente para evitar su identificación, según advierten los expertos informáticos.

Los programas tienen un aspecto diverso: algunos introducen por su cuenta y riesgo un "favorito" en la lista correspondiente; otros incluyen barras de navegación o colocan una página inicial -la que aparece al abrir el explorador de Internet- diferente a la que instaló originalmente el usuario.

Los más dañinos son capaces de capturar lo que el usuario teclea, incluso nombres de usuario y contraseñas.-

¹³ Ver "Riesgo Informático- Nueva modalidad a través de Internet: 'Phishing'".

¹⁴ <http://www.phillyburbs.com/pb-dyn/news/103-10232004-388338.html>

¹⁵ http://www.spywareguide.com/product_show.php?id=953