

## 1. Phishing: El robo de identidad

Se conoce como “Phishing” a la estafa o fraude que utiliza medios electrónicos con el objetivo de suplantar la identidad. Gracias a esta práctica, el estafador puede hacerse con información privilegiada, como datos bancarios o contraseñas, entre otros.

Etimológicamente, el término Phishing procede del inglés “fishing”, que significa “pesca”. Se entiende que el delincuente “pesca” a un usuario mediante engaños para obtener su información. En nuestra ya costumbre de adoptar las voces inglesas para los términos informáticos, la persona que practica Phishing es conocida como *phisher*.

El Phishing es una práctica englobada en el movimiento conocido como Ingeniería Social. En el ámbito informático, la Ingeniería Social es un concepto que refiere a obtener información confidencial recurriendo al engaño del usuario del sistema de cómputo.

Un sistema de cómputo es el conjunto de elementos que permiten el funcionamiento de un entorno informático. Estudiado este sistema a cualquier nivel de profundidad, en un extremo encontramos al hardware (elementos físicos y electrónicos del ordenador) y en el extremo opuesto al usuario (la persona que utiliza el ordenador).



Figura 1. El sistema de cómputo

\* Ingeniero Técnico en Informática y profesor de informática del IES Francesc Ribalta.

Ribalta. *Quaderns d'aplicació didàctica i investigació*, núm. 14 (deseembre 2008), ps. 153-164.  
 © IES Francesc Ribalta · Castelló de la Plana · ISBN: 978-84-691-7720-4  
<http://www.iesribalta.net/revista>

Si la práctica de delitos informáticos conocida como hacking (o cracking) es un ataque a los eslabones del hardware y el software en el sistema de cómputo, las prácticas de Ingeniería Social utilizan la inocencia del usuario para poder incidir en el sistema.

### Funcionamiento

Aunque hay distintas formas de practicar Phishing, normalmente se lleva a cabo a través de estas cuatro fases:

**1. Envío de correos electrónicos.** El phisher utiliza programas para enviar automáticamente millones de correos electrónicos a los usuarios que pretende pescar. Normalmente, el phisher envía los correos simulando que es una empresa conocida por el usuario, como por ejemplo, su banco. Se hace creer al usuario que los correos son legítimos.

**2. El usuario confía.** El usuario, que cree que el correo procede realmente de su entidad bancaria, realiza un acto de confianza y responde. En casi todos los casos, el correo contiene un vínculo o enlace Web cuyo objetivo es dirigir al usuario a la página Web del phisher (donde se llevará a cabo la “pesca”).

La estrategia comúnmente utilizada es notificar al usuario que debe actualizar los datos de su cuenta. El usuario cree que debe facilitar sus datos para que su perfil bancario o de correo sea actualizado.

**3. El usuario accede a la Web del phisher.** El usuario confía y hace clic en el enlace Web. A continuación, el usuario accede a la Web del phisher, que no es más que una copia exacta y falsa de la Web original de la empresa a la que se cree estar accediendo. Por ejemplo, un phisher que desee realizar una estafa a través de Bancaja, diseñará una página Web exactamente igual que *www.bancaja.es* para que el usuario crea estar en la Web de su banco.

Aquí comienza la pesca. El usuario introduce sus datos personales, que en realidad están siendo almacenados en una base de datos propiedad del phisher. Entre estos datos pueden incluirse datos personales, direcciones, teléfonos, datos bancarios, contraseñas de cuentas bancarias e incluso el número de la seguridad social. Ahora el phisher dispone de la información robada.

**4. Se produce el robo de dinero.** Gracias a los datos obtenidos y con ayuda de cuentas bancarias de intermediarios, el phisher realiza transferencias bancarias y se hace con el dinero del usuario.

### *Perjuicios del Phishing*

Entre los daños que produce el Phishing podemos encontrar:

**1. La pérdida inherente de dinero.** El perjuicio más grave de todos, sin duda. Dado que esta práctica nace en los Estados Unidos, es allí donde se registran las escalofriantes pérdidas económicas de los usuarios.

La firma de investigación de mercado y nuevas tecnologías americana Gartner (<http://www.gartner.com>) señala en uno de sus informes que el Phishing sustrajo 3.200 millones de dólares en los Estados Unidos durante septiembre de 2006 y agosto de 2007. En este periodo, se calcula que fueron estafados más de 3 millones de usuarios, engañados con una media de unos 800 dólares por persona.

En 2008 la cosa no ha mejorado. Un reciente estudio del órgano Anti-Phishing Work Group redacta que los intentos de Phishing en 2008 han triplicado a los del año anterior.

**2. La pérdida del acceso a medios.** El usuario puede perder la posibilidad de acceder a su cuenta de correo electrónico o incluso a plataformas digitales de carácter económico como PayPal, que es un medio que también está directamente relacionado con la cuenta bancaria del usuario y desde el cual se puede acceder al dinero del mismo.

### *Cómo prevenir el Phishing*

El Phishing es una estafa y puede prevenirse si el usuario es conocedor de ciertos aspectos referidos a la navegación Web. Algunas medidas recomendadas para prevenir ataques de Phishing son:

**1. No responder a solicitudes de información privilegiada si son enviadas a través de correo electrónico.** El banco y otras empresas reconocidas jamás utilizarían el correo electrónico para comunicarse con clientes en caso de necesitar información de este tipo.

**2. Visitar una página Web introduciendo la dirección en la barra de direcciones.** No se debe acceder a la Web del banco (o empresa implicada) a través de enlaces de otras Webs ni enlaces de su correo electrónico. Si se utiliza la barra de direcciones, se accederá a la Web principal y se evitará terminar en la Web del phisher.

En algunos casos, visualizar el dominio en la barra de direcciones podría ser suficiente para detectar el Phishing, ya que algunos phishers no consiguen clonar el dominio completo de la Web de su banco. Hay que tener cuidado, no obstante, con los nombres de dominio que parecen idénticos, pero que no lo son. En algunos tipos de letra, hay caracteres muy parecidos o iguales, como por ejemplo el número uno y la letra ele minúscula, o la letra o minúscula y la griega ómicron.

**3. No introducir datos privilegiados en sitios Web sin cifrado.** El cifrado de datos, representado en muchos navegadores con el dibujo de un candado, afirma que el sitio Web está implementado para la segura protección de datos que se introducen en él.



Figura 2. Indicación de candado en Internet Explorer

Un sitio Web sin cifrado no es un lugar seguro para introducir datos. Haciendo doble clic sobre el icono del candado, se puede acceder a comprobar el certificado de seguridad con el que funciona el sitio. Si su navegador le anuncia que el certificado utilizado no se reconoce, es posible que se encuentre en un sitio falso o no seguro.

**4. Consultar frecuentemente su saldo bancario.** Permanecer atento a los movimientos de sus cuentas bancarias y tarjetas le permitirá detectar a tiempo cualquier transacción sospechosa y actuar.

#### *Cómo solucionar el Phishing*

Esta práctica no sólo tiene medidas preventivas, sino que también se enfrenta a una serie de soluciones que contribuyen a su futura erradicación.

**1. Educación Anti-Phishing.** Como práctica de Ingeniería Social que se apoya en la inocencia del usuario para llevar a cabo la estafa, la solución directa es concienciar y educar a los usuarios sobre el Phishing y otras técnicas para evitar que los “ingenieros sociales” puedan engañarles. Si todos los usuarios de Internet fueran plenos conocedores del funcionamiento de estas estrategias, se convertirían en prácticas poco o nada efectivas.

Para ello han nacido órganos como APWG (Anti-Phishing Work Group), que se encarga de informar y educar a la sociedad en cuanto a medidas para combatir el Phishing.

Otras empresas reconocidas, como Microsoft, facilitan material gratuito con medidas preventivas y soluciones.

**2. Mejorar el Software.** Es posible mejorar ciertos programas para que el Phishing sea menos efectivo. Actualmente, navegadores Web como Mozilla Firefox son capaces de detectar un buen número de Webs falsas y disparan una alerta al usuario antes de que éste tenga tiempo de introducir su información.

**3. Denuncia.** El Phishing es un fraude penado por la ley y como tal puede ser denunciado. Facilitar a la empresa implicada toda la información acerca del phisher como los correos recibidos o detalles sobre las fechas de los robos, ayudará a las autoridades competentes a dar con el estafador.

#### *El futuro del Phishing*

A pesar de las estafas mediante Phishing aumentan en poco tiempo a un ritmo vertiginoso, el órgano APWG vaticina un futuro incierto para esta práctica tal y como se la conoce en la actualidad. No obstante, insisten en que la estrategia de estafa a través de la red que sobrevivirá será el denominado *Pharming*.

La práctica del Pharming consiste en encontrar fallas en el sistema de nombres de dominio (DNS) con el fin de redirigir al usuario a la Web del phisher aunque éste haya introducido la URL de la página Web en la barra de direcciones. Sin duda, una táctica más eficaz y difícil de detectar.

## 2. Spam: Correo no deseado

El spam es una estrategia que consiste en enviar correos electrónicos sin la autorización previa del destinatario. A estos correos se les conoce también como “correos no deseados” o “correos basura”. El spam se realiza con fines publicitarios o de ingeniería social y en España su práctica está sancionada por la ley<sup>1</sup>.

El envío masivo de correos basura es la estrategia utilizada por los phishers para propagar sus falsos mensajes. Los mensajes enviados son amigables y atractivos para conseguir que el usuario los lea y acceda a sus contenidos. Entre estos falsos mensajes podemos encontrar:

- 1. El dinero fácil.** Se tienta al usuario con falsos premios económicos, falsas ofertas de empleo o engañosas estrategias para obtener dinero fácil en apuestas, loterías o casinos.
- 2. Material erótico.** Se pretende engañar sobre enlaces con fotos de personajes famosos.
- 3. Falsos registros.** Se envía al usuario un correo informando de que su cuenta en una Web o portal ha de ser revisada o actualizada, cuando en realidad no existe tal cuenta.

### *La obtención de cuentas de correo*

Las empresas dedicadas al spam disponen de millones de direcciones de correo electrónico existentes a pesar de que éstas forman parte de bases de datos restringidas y son propiedad de sus propietarios. Hay varias maneras de obtener cuentas de correo para propagar correo basura:

**1. Tráfico de datos.** Un usuario de Internet suele facilitar su cuenta de correo en diversas plataformas tales como comunidades, compras en tiendas online, compra de billetes de avión o tren, solicitud de presupuestos a comercios, solicitud de información, etc. En la teoría, esta información es restringida, y no es usada para fines maliciosos, además de que no es facilitada a otras empresas.

A pesar de ello, existen empresas que recopilan las cuentas en una base de datos, procediendo después a la traficación. De esta manera, las empresas interesadas obtienen un listado con millones de cuentas de correo y proceden a la divulgación del correo basura.

**2. Mensajes cadena.** Un mensaje cadena es un correo electrónico que pretende que el destinatario lo reenvíe en masa a toda su agenda de contactos.

Para que el usuario se vea empujado a continuar la cadena de mensaje con todos sus conocidos, se suele recurrir a la difusión de mentiras o bulos (acción popularmente conocida como Hoax<sup>2</sup>). Un ejemplo podría ser “El MSN Messenger se convertirá en software de pago si no envías este mensaje a todos tus conocidos” o “Si envías este mensaje a 100 personas tendrás un año de buena suerte”. Estas

---

1. La LEY 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, establece en su artículo 21 la prohibición del envío de publicidad a través de medios electrónicos sin autorización expresa del destinatario. En el apartado a) del artículo 39 de la misma ley, consta que la sanción económica para el delincuente en caso de una infracción muy grave podría ascender a 600.000 euros.

2. Hoax, del inglés: Bulo, engaño.

cadenas son realmente difundidas por el público joven y adolescente, escondiendo un peligroso tráfico de información en lo que aparenta ser un inocente juego entre niños.

Cuando un usuario envía un mensaje a múltiples destinatarios, tiende a utilizar el campo “Destino” para introducir las cuentas de correos. De este modo, las cuentas de correo a las que ha sido enviado el mensaje son visibles desde cada una de las cuentas destino. Esto produce una creciente bola de nieve que contiene los correos destinatarios de cada uno de los envíos anteriores, formando una visible masa de cuentas de correo electrónico que será recolectada por una empresa spammer.

#### *Soluciones para menguar el efecto spam*

Para paliar la corriente de correo basura, existen soluciones software y del propio usuario que se pueden llevar a cabo:

**1. Filtro antispam.** Algunos gestores de correo electrónico disponen de filtros que pretenden detectar los mensajes de spam y desplazarlos automáticamente a un directorio de “correo no deseado”. El usuario puede ayudar al filtro, marcando como “spam” los mensajes que el filtro no pueda detectar.



Figura 3. Filtro antispam de Gmail

**2. No abrir los correos basura.** La mayoría de estos correos son reconocibles sin tan siquiera proceder a su lectura detallada. Educando a los usuarios de Internet se puede conseguir que éstos detecten la mayoría de los mensajes de spam y los ignoren o eliminen.

**3. Realizar envíos múltiples con Copia Oculta (CCO).** Al enviar correos a múltiples destinatarios, pueden escribirse las direcciones en el campo “CCO” en lugar de en el campo de “Destino” o “CC”. Esta acción produce un efecto de ocultación: a ojos del destinatario, el correo ha sido enviado a él, únicamente. De esta manera se contribuye a reducir la divulgación innecesaria de direcciones.

### 3. Spyware: Espionaje a través de Internet

El devastador envío de spam no ha sido utilizado únicamente con fines publicitarios, sino que ha sido el punto clave para colarse en los ordenadores de los usuarios y estudiar sus movimientos, violando así los derechos de privacidad e iniciando toda una red de “espionaje informático”.

El espionaje se lleva a cabo normalmente a través de Spyware. El término “Spyware”, que procede de las inglesas “spy” (espiar) y “software”, puede denominarse en castellano como “programas espía”.

Un programa espía es una aplicación informática que se instala en un ordenador y recopila información sobre el usuario sin su conocimiento.

Algunas de estas aplicaciones se presentan en forma de software publicitario, ventanas publicitarias que aparecen automáticamente aunque no se esté navegando, o incluso barras de herramientas adicionales en los navegadores Web. Estas últimas se conocen como “toolbar”, que en inglés significa “Barra de herramientas”.



Figura 4. La Toolbar de Google

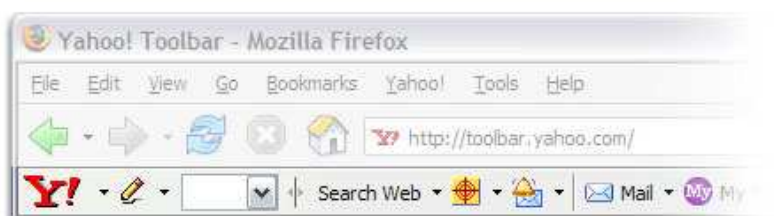


Figura 5. La Toolbar de Yahoo!

#### *Funcionamiento*

- 1. El usuario contrae el Spyware.** La aplicación maliciosa puede colarse en el ordenador a través de un mensaje de spam o puede estar contenido en software descargado de Internet. Es posible que un programa gratuito venga acompañado de un programa espía en un sitio Web no seguro; el usuario ignora este hecho, e instala la aplicación en su ordenador.
- 2. El Spyware recopila información.** El programa reúne datos sobre el usuario. Se recogen datos como las páginas Webs visitadas, las palabras que se introducen en los motores de búsqueda, las descargas efectuadas e incluso la introducción de datos en sitios Web.
- 3. El Spyware envía la información.** El programa envía los datos a la empresa interesada de manera ininterrumpida. Los programas espía no sólo recopilan

información de manera ilegal, sino que además utilizan los recursos de red del propio ordenador, consumiendo ancho de banda y contribuyendo al mal funcionamiento de la máquina.

#### *Espionaje en los navegadores Web*

Los sitios Web o herramientas como los motores de búsqueda, como el archiconocido Google, pueden almacenar un registro sobre las búsquedas realizadas por un mismo usuario. Esta práctica se realiza a través de las cookies<sup>3</sup> del navegador Web para mejorar la calidad de las visitas reincidentes: el usuario normalmente desea conocer los sitios que ha visitado y los que no, además de las palabras clave que ha utilizado.

El problema es que estas ventajas se traducen a un estudio de los movimientos del usuario para beneficio de las empresas que recopilan información. Con la información obtenida, las empresas pueden amoldar la información a las tendencias de cada usuario, emitiendo una publicidad personalizada, acorde con las tendencias individuales del internauta.

#### *Solucionar el problema del Spyware*

Las aplicaciones de Spyware son aplicaciones maliciosas que en algunos casos pueden ser erradicadas del ordenador.

**1. Programas antivirus.** Existen aplicaciones espía que son detectadas por el antivirus y que pueden ser eliminadas tras un escaneo rutinario. Además existen aplicaciones especializadas en la búsqueda de espías, como el gratuito Ad-Aware (<http://www.lavasoft.com>).

**2. Revisar las cookies.** Revisar y eliminar las cookies del navegador, e incluso desactivarlas, evita que éste recoja información sobre los hábitos del usuario. El problema de esta solución es que se prescindirán de las ventajas de las cookies.

**3. No descargar software sospechoso o de sitios no seguros.** El software gratuito ha de descargarse de los sitios Web oficiales, e incluso en ese caso, se ha de revisar que no se está descargando o instalando alguna aplicación adicional de este tipo que el programa pueda contener.

---

<sup>3</sup> Las cookies son archivos que el navegador Web almacena automáticamente con cada visita a un sitio Web. Las cookies pueden ser configuradas, desactivadas, revisadas y eliminadas por el usuario en cualquier navegador Web.

#### 4. Educar para el buen uso de Internet

Una vez analizadas a fondo las estafas de Internet, sus causas, sus síntomas, sus consecuencias y sus soluciones, es interesante analizar el uso que se le da a Internet en nuestro país actualmente.

Según estudios recientes realizados por el Instituto Nacional de Estadística, el 76,8% de los niños de entre 10 y 15 años accedieron a Internet en el último trimestre de 2007. Además, el 64,7% de los niños de la misma edad eran dueños de un teléfono móvil durante la misma fecha (medio a través del cual también se procede a estafas parecidas al spam y al Phishing).

En el caso concreto de la Comunidad Valenciana, se supera la media, encontrando que el 90,5% de los niños de 10 a 15 años han sido usuarios de Internet en el último trimestre de 2007.

Total Niños (10 a 15 años)	Niños usuarios de Internet (Tercer trimestre 2007)	Niños que disponen de teléfono móvil
2.497.163	76,8%	64,7%

Figura 6. Uso de Internet y móvil de niños de 10 a 15 años

Territorio	Niños usuarios de Internet				Niños con teléfono móvil			
	2004	2005	2006	2007	2004	2005	2006	2007
España	68%	72%	75,8%	76,8%	45,7%	54,3%	57,7%	64,7%
Comunitat Valenciana	64,8%	69,7%	72,8%	90,5%	49,2%	58,8%	58,4%	65,1%

Figura 7. Evolución del uso de Internet y móvil de niños de 10 a 15 años desde 2004 a 2007

Aprender a utilizar las TIC no es sólo un objetivo que se ha marcado en la educación del país; el aprendizaje de informática está presente en adultos que de manera voluntaria asisten a cursos o talleres de informática. Según los datos ofrecidos por el INE, el 63,5% de las personas de más de 16 años ha asistido, al menos, a un curso de informática por cuenta propia.

Edad	Total personas	Han realizado un curso de informática		Nunca han realizado un curso de informática
		Entre 2005 y 2007	Antes de 2005	
Todos	21.496.273	35,1%	28,4%	36,5%
16-24 años	4.338.957	37,9%	30,1%	32,0%
25-34 años	6.467.233	39,3%	21,6%	39,1%
35 años o más	10.690.083	34,3%	28,6%	37,1%

Figura 8. Asistencia a cursos de informática de personas mayores de 16 años, por momento de realización del curso

En conclusión, la educación es una clave fundamental para combatir los fraudes de ingeniería social que utilizan al usuario como punto débil del sistema de cómputo. Formando a los usuarios en el buen uso de Internet e invitándoles a conocer a fondo todos estos delitos, su éxito se verá reducido.

A continuación se proponen una serie de actividades para trabajar en el aula de informática y conseguir que los alumnos conozcan a fondo el Phishing, el Spyware y el spam.

## 5. Trabajo en el aula de informática

### *Actividad 1: Cómo prevenir y solucionar el Phishing*

Una vez conocido el concepto de Phishing, los alumnos se dividirán en grupos de tres. Ayudándose de Internet deberán anotar todas las ideas relacionadas con los siguientes puntos:

Proponer medidas para prevenir el Phishing

Proponer medidas para solucionar el Phishing.

Encontrar plataformas Web concretas en las que se podría producir Phishing a usuarios españoles.

Después de anotar todas las ideas, se expondrán a toda la clase con el objetivo de realizar un informe común que resuma las propuestas más importantes de la sesión. Los alumnos deberán redactar de forma conjunta un documento, a modo de guía o de folleto informativo que reúna toda la información desarrollada y que sirva como apoyo a cualquier interesado que quiera conocer más acerca de las estafas a través de Internet.

No sólo pueden redactar las ideas, también es recomendable reunir material gráfico como capturas de pantalla de páginas Web.

El documento podrá ser descargado desde Internet, por ejemplo, desde un espacio personal del centro, como recurso educativo, desde la Web del centro o desde una Web o Blog del alumnado.

#### *Actividad 2: Aprender a detectar el Spyware*

Esta actividad consiste en que los alumnos descarguen e instalen en el ordenador una serie de aplicaciones gratuitas de uso doméstico. Los alumnos deberán buscar la aplicación con un motor de búsqueda, y encontrarla en al menos cinco sitios Web diferentes. Se deberá realizar un documento para cada programa y Web en el que se anote:

1. Web donde se ha encontrado.
2. ¿Contiene aplicaciones adicionales? Sí/No
3. ¿Qué funciones realizan las aplicaciones adicionales?
4. ¿Cuánto espacio en MB ocupan las aplicaciones adicionales?
5. ¿Estas aplicaciones pueden ser instaladas voluntariamente o son impuestas con el software?
6. ¿Qué problemas crees que pueden presentar en tu PC estas aplicaciones?

Algunos de los programas que pueden proponerse para descarga son:

1. Navegadores Web: Mozilla Firefox, Opera.
2. Reproductores de vídeo/audio: Winamp, BS Player, VLC Player.
3. Paquetes de codecs: K-Lite.
4. Mensajería instantánea: MSN Messenger.

#### *Actividad 3: Correo con Copia Oculta*

En esta actividad los alumnos aprenderán a utilizar la copia oculta de su gestor de correo electrónico. Deberán enviar un mensaje anunciando la URL donde poder descargar el informe anti-phishing que han redactado.

Para ello, escribirán la dirección de sus compañeros de clase en el campo "CCO" y la suya propia en el campo "Destino", para evitar que los destinatarios visualicen las demás direcciones.

#### *Actividad 4: Análisis comparativo de Webmail*

Esta actividad ayudará a los alumnos a reflexionar sobre los distintos Webmail y escoger uno más adecuado, teniendo en cuenta todo lo conocido sobre el concepto de correo no deseado, Spyware y Phishing.

Los alumnos deberán crear una cuenta de correo en al menos tres Webmail distintos, como por ejemplo, Gmail, Hotmail y Yahoo. Deberán realizar un análisis comparativo y anotar las conclusiones teniendo en cuenta criterios como:

- ¿Utiliza filtro antispam? ¿Es efectivo?
- ¿Permite detectar visualmente un correo no deseado antes de ser leído o abierto?
- ¿Dispone de sistema antivirus para los archivos adjuntos?
- ¿Realiza acciones que pueden llevar a la apertura involuntaria de correos spam, como por ejemplo, la apertura automática de mensajes?

## Bibliografía

- APWG (2008): *Phishing Activity Trends Report January-March 2008*, <<http://www.antiphishing.org>> [Consulta: 28 de Octubre de 2008]
- BOE (2002): *LEY 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico*, Madrid, <<http://www.boe.es>> [Consulta: 25 de Octubre de 2008]
- Cabanillas, M (2007): "Aumento considerable de los ataques de phishing en 2007", *Revista PC World Digital*, IDG Communications, Madrid. <<http://www.idg.es/pcworld>> [Consulta: 25 de Octubre de 2008]
- Conselleria de Cultura, Educació i Esport (2006): *El buen uso de Internet*, Generalitat Valenciana.
- Instituto Nacional de Estadística (2008): *Asistencia a cursos de informática por características demográficas y momento de realización del último curso*, Madrid, <<http://www.ine.es>> [Consulta: 04 de Noviembre de 2008]
- Instituto Nacional de Estadística (2008): *Encuesta sobre Equipamiento y Uso de Tecnologías de la Información y Comunicación en los hogares 2007*, Madrid, <<http://www.ine.es>> [Consulta: 04 de Noviembre de 2008]
- Instituto Nacional de Estadística (2008): *Evolución de datos de Niños de 10 a 15 años (2004-2007) por Comunidades Autónomas*, Madrid, <<http://www.ine.es>> [Consulta: 04 de Noviembre de 2008]
- Microsoft (2004): *Todo lo que debe saber acerca del "phishing"*, Madrid. <<http://www.microsoft.com>> [Consulta: 27 de Octubre de 2008]
- Reischl, G (2008): *El engaño Google*, Medialive Content S.L.
- Silberschatz, A, Galvin, P y Gagne, G. (2004): *Sistemas Operativos (6ª Edición)*, Limusa.