Educación, medios de comunicación y Web 2.0: Presente y futuro
Madrid 26-30 de abril de 2010

Ponencia

La seguridad en Internet

Jorge López Werner
Jefe del Dpto. de Informática e Innovación Tecnológica
Instituto de Tecnologías Educativas
Ministerio de Educación de España

Índice

La informática en el entorno escolar y en el hogar..... pag. 2
Redes de datos en centros escolares
Acceso a Internet en los centros docentes
Acceso a Internet en el hogar

Aspectos generales de la seguridad en Informática..... pag. 6
Riesgos en la seguridad de los equipos informáticos..... pag. 7
Riesgos en la navegación por Internet..... pag. 9

Sistemas de protección..... pag. 14
Sistemas de protección local..... pag. 14
Sistemas de protección perimetral y navegación segura..... pag. 14
Sistemas de control parental..... pag. 16
Sociología de la seguridad..... pag. 16

Consejos para minimizar los riesgos en la navegación por Internet..... pag. 19

Enlaces de interés..... pag. 22

La informática en el entorno escolar y en el hogar

Desde el año 1985 se llevan incorporando ordenadores a los centros escolares, siguiendo dos patrones claramente diferenciados:

Por un lado, la integración de ordenadores destinados a tareas de gestión escolar, la administración de alumnos, calificaciones, comedores escolares, gestión económica de los centros y demás tareas administrativas relacionadas directa o indirectamente con las anteriores.

Por otro lado, la aportación de equipamiento informático para apoyo a la tarea docente, como herramienta en el proceso de enseñanza-aprendizaje, siguiendo tres paradigmas diferentes de integración por todos conocidos: aulas de ordenadores, el ordenador en el aula y actualmente, el modelo uno a uno de integración, con un ordenador personal para cada alumno y orientado para un uso mixto del mismo, tanto en el aula como en el hogar.

Así mismo, la informática educativa parte de la colocación, en los primeros estadios de implantación, de conjuntos de equipos aislados, sin conectividad externa, salvo por el uso de soluciones de conectividad individual, normalmente modems en los equipos de dirección y/o administración, sobre líneas RTB, para el acceso a servicios BBS y posteriormente a Internet.

Paralelamente, en el entorno empresarial, partiendo de los despliegues realizados por las grandes corporaciones y alcanzando progresivamente a la mediana y pequeña empresa, se despliegan redes de datos, inicialmente coaxiales y posteriormente redes de cableado estructurado tipo Ethernet, que son las que actualmente tenemos desplegadas.

En el ámbito escolar, normalmente motivado por el elevado coste de las inversiones a realizar, las redes de datos se circunscriben a las aulas de informática que se complementan con soluciones de conectividad inicialmente vía RDSI y posteriormente a través de líneas ADSL, con las que se facilita la conexión de todos los equipos de un mismo aula a Internet.

Tan sólo en algunas zonas muy localizadas geográficamente, se aportan soluciones integrales de conectividad a los centros, como en el caso de los centros escolares públicos de Ceuta y Melilla donde a partir del año 2000 se realizan tendidos de cableado estructurado de red, tipo Ethernet, cubriendo con ellos el 100% de las dependencias del centro, de manera que llegue a cada aula, al menos un punto de red. Estas redes, cuyo despliegue se finalizó en 2006, si bien se siguen realizando actuaciones de ampliación y mejora para adecuarlas a las nuevas necesidades, permiten que haya conectividad a Internet desde cualquier lugar del centro, y por ello exigen tener en cuenta una serie de consideraciones en cuanto a seguridad que abordaremos más adelante.

En determinadas regiones como la Comunidad Autónoma de Extremadura se hacen igualmente despliegues de red integrales en los centros, en este caso asociados así mismo a la integración de un equipo informático fijo por alumno en cada aula, con cambio incluso del mobiliario preexistente por otro mejor adaptado.

Paralelamente y al amparo de programas institucionales se producen despliegues de redes inalámbricas en centros educativos, normalmente del tipo 802.11 b y g. Tal es el caso de los Institutos de Educación Secundaria de la Comunidad Murciana y de otras Comunidades Autónomas, del estado español.

La aplicación de programas de integración de las TIC en el entorno escolar siguiendo el modelo de integración uno a uno, como el Magallanes en Portugal y el Escuela 2.0 en España plantean la necesidad de dotar de un sistema mixto de conectividad en los centros educativos, en el que se combinen soluciones de cableado estructurado de datos con sistemas de conectividad inalámbrica, añadiendo elementos de complejidad a la conectividad en sí misma así como a los aspectos de seguridad que se derivan de ella.

Atendiendo a la clasificación de los medios tecnológicos informáticos introducidos en el entorno escolar según su funcionalidad, podremos así mismo establecer los niveles de criticidad de los mismos en cuanto a su operatividad, y la seguridad a aplicar en los mismos.

Los sistemas informáticos destinados a las tareas administrativas contienen normalmente bases de datos con información de los alumnos, informaciones de acceso a cuentas bancarias, DNI, direcciones, teléfonos, es decir, todos aquellos datos que están obligatoriamente protegidos por las normativas de protección de datos de los respectivos países. En España, la Ley Orgánica 15/1999 de 13 de diciembre de Protección de Datos de Carácter Personal, conocida como LOPD, según la cual, el titular de la base de datos tiene la obligación de custodia sobre los mismos, así como de garantizar los derechos de acceso, rectificación y cancelación, y por tanto es responsable de aplicar las medidas de seguridad necesarias para evitar el robo y/o la cesión a terceros de los mismos sin consentimiento precio de los interesados.

Estas consideraciones anteriores nos marcan un nivel de criticidad elevado en cuanto a seguridad se refiere en este tipo de dispositivos informáticos.

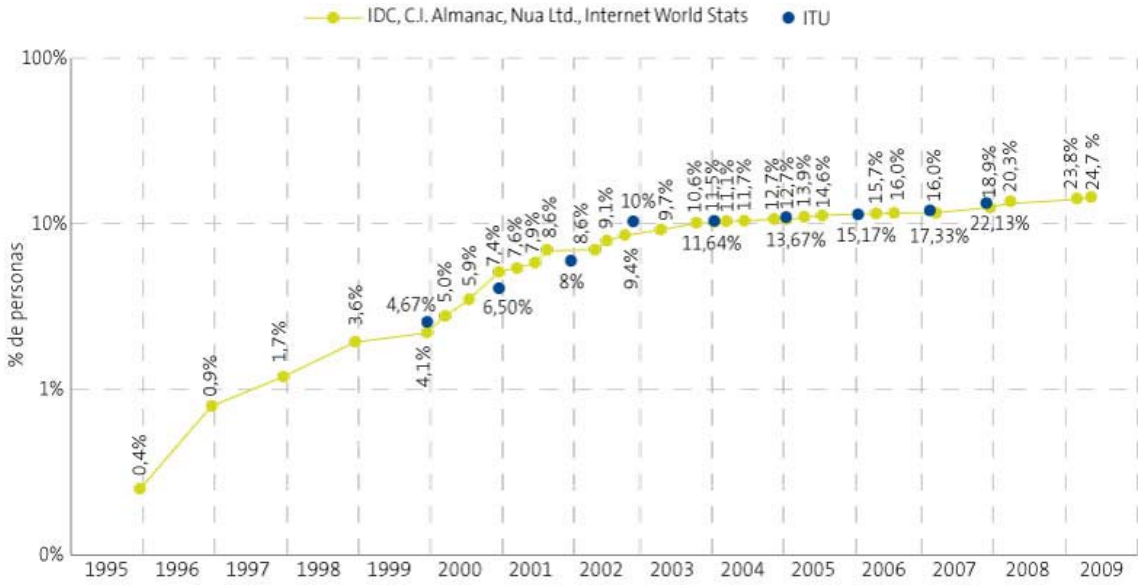
Evidentemente, los sistemas informáticos destinados a ejercer la función de herramientas para el uso didáctico no deberían contener datos sensibles. En el caso de estos sistemas, la criticidad viene derivada fundamentalmente de la necesidad de mantenerlos operativos el mayor tiempo posible y no tanto el protegerlos desde el punto de vista de los datos que residen en ellos.

Por el contrario, sí resulta vital garantizar que el acceso a determinados contenidos en ellos esté protegido para evitar el acceso a sitios Web con contenidos pornográficos, violentos, sexistas, de apuestas o que atenten contra la moral y la salud del alumnado.

Al ser la problemática diferente, las soluciones a aplicar también son distintas, como veremos más adelante.

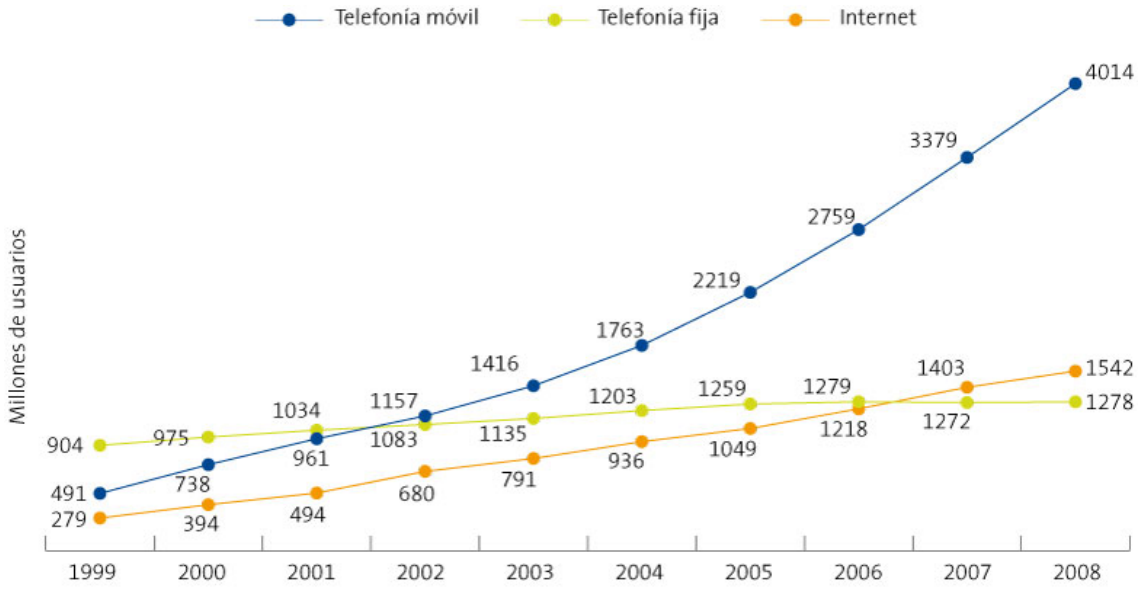
Paralelamente a la integración de las TIC en el entorno escolar, se ha producido un desarrollo importantísimo en los últimos 10 años en cuanto a la utilización por parte de los ciudadanos tanto del uso de los ordenadores y la telefonía móvil como del acceso a Internet.

Si atendemos a datos estadísticos, escogidos del informe anual de Fundación Telefónica sobre la Sociedad de la Información, y de los informes PISA y de la OCDE, la evolución en el incremento de internautas a nivel mundial desde 1995 a 2009 ha sido espectacular.



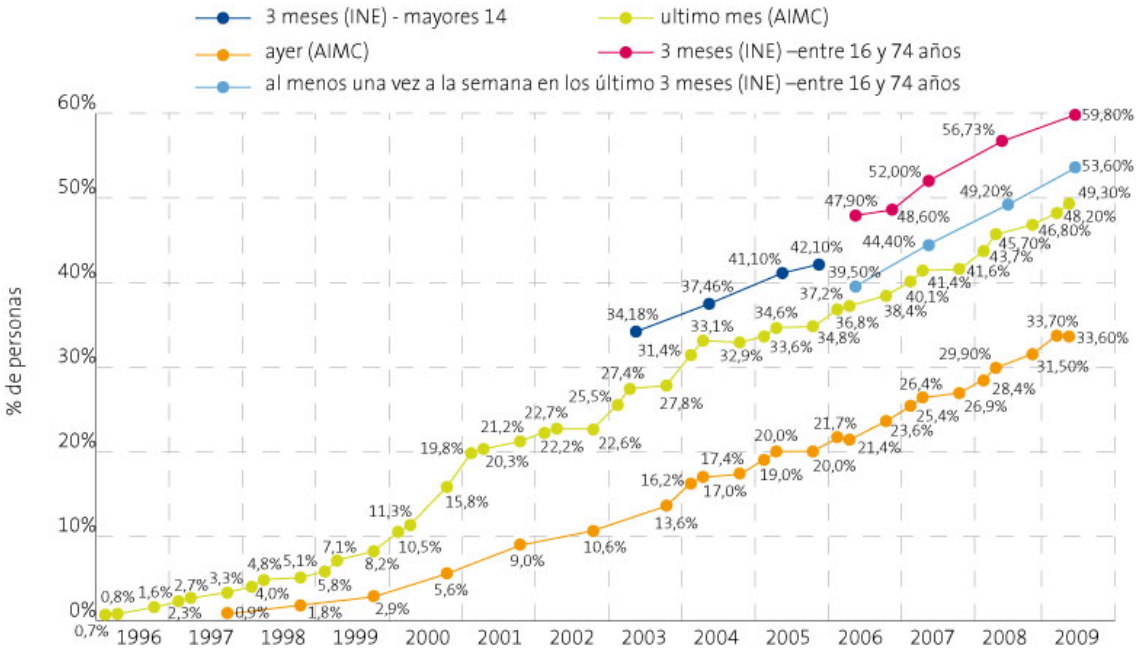
Como se puede observar, el incremento es sostenido en el tiempo, si bien el momento álgido de crecimiento se produce en torno al año 2000, en el que Internet deja de ser utilizado por una minoría y pasa a generalizarse.

Comparativamente, respecto a la implantación de la tecnología más utilizada para las comunicaciones, podemos comprobar que el dispositivo preferido para comunicarse es el teléfono móvil:

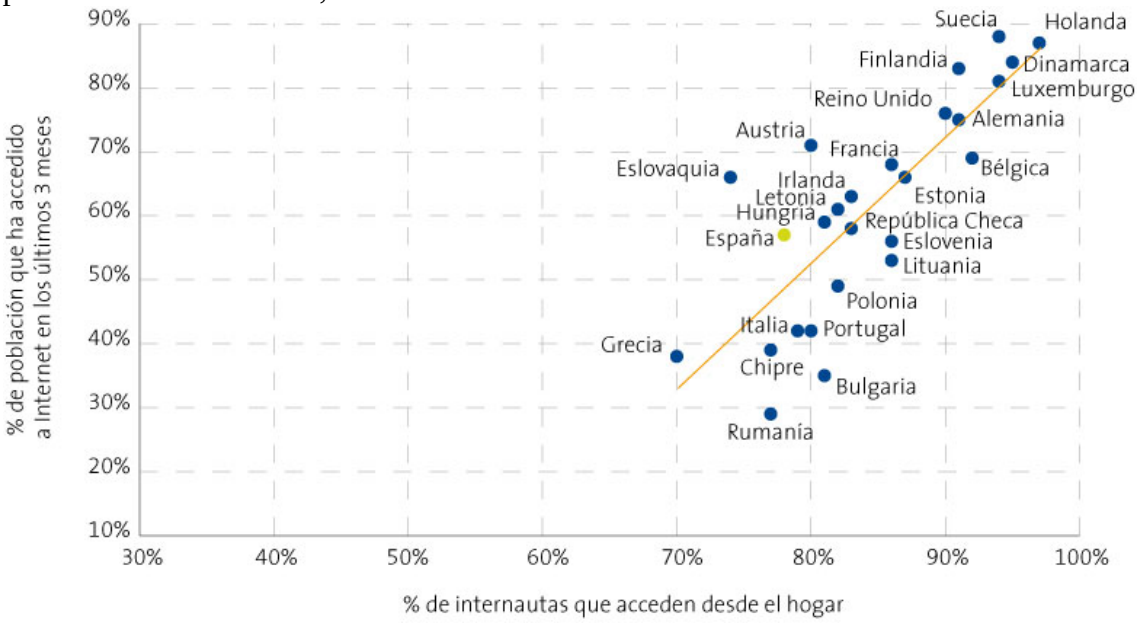


El número de usuarios que prefieren esta plataforma de comunicación es significativamente mayor incluso que los que usan Internet, Aun así, hay que tener en cuenta que la tendencia general es converger hacia el acceso a las redes e Internet desde los dispositivos de telefonía móvil, cada vez más sofisticados.

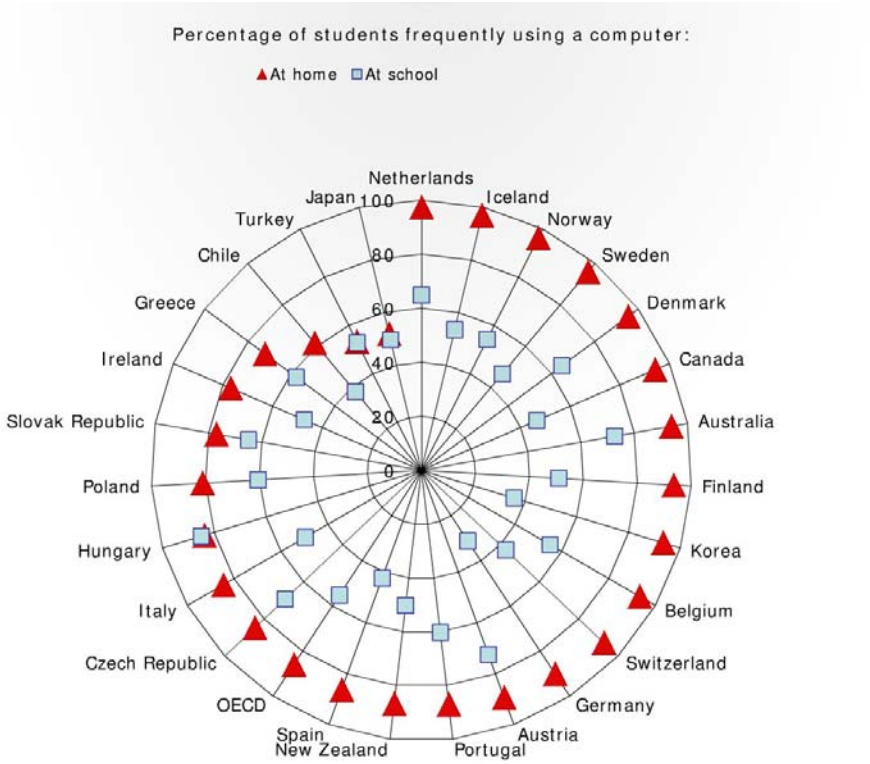
Descendiendo al nivel de España, el grado de penetración de Internet en la sociedad es significativamente más alto que la media mundial, si bien en el año 2008 aún nos encontramos por detrás de los 20 países más desarrollados:



De este número significativo de internautas, en España, cerca del 60% lo hacen desde el hogar, lejos del casi 90% de penetración en los hogares que tiene Internet en países próximos como Holanda, Suecia o Dinamarca.



Curiosamente, si comparamos los datos de acceso en el hogar con el acceso a Internet desde las escuelas, en casi todos los países se producen diferencias significativas a favor del acceso desde los hogares, siendo especialmente diferente el nivel de utilización en países como España, Canadá, Alemania:



Evidentemente, todo este volumen de datos acerca de la tecnología, su grado de implantación tanto a nivel social como escolar y la localización del lugar desde donde se produce el acceso a Internet, nos permite focalizar los problemas de seguridad que de ellos se derivan y nos orientan en el lugar y manera de orientar y aplicar las posibles soluciones.

Aspectos generales de la seguridad en Informática

Evidentemente, el problema de la seguridad en los sistemas de datos e información ha sido una preocupación desde los orígenes de estos sistemas.

De hecho, si atendemos al propio origen de los sistemas informáticos, encontramos que parte de sus raíces modernas se encuentran en la necesidad de desencriptar mensajes en tiempos de preguerra y guerra entre las potencias de la época, rondando los años 40 del siglo XX.

El Collosus, construido por Turing con la ayuda de Von Neuman, fue el primer ordenador operativo cuyo cometido era vulnerar los mensajes encriptados por la famosa máquina Enigma con la que los alemanes codificaban sus mensajes de guerra.

Sin embargo, apartando estas escenas románticas de película, el problema de la seguridad en los sistemas de computación se limitan a controlar el acceso a las personas a los sistemas así como a garantizar que éstas no divulguen sus claves de acceso, hasta bien entrada la década de los 80.

El primer virus informático surge casi como un juego de estudiantes. En el año 1982, Rich Skrenta, con tan sólo 15 años de edad, crea “Elk Cloner”, un pequeño programa

que se copia en las unidades de disquete sin permiso de los usuarios y a través de su inserción en los diferentes equipos por los que va pasando. Su efecto es igualmente romántico, pues el fin de Skrenta es distribuir un pequeño poema indicando que había infectado el ordenador.

Paralelamente, es en esa época cuando se empieza a hablar de códigos autorreplicantes, siendo en 1983 cuando se introduce por primera vez el término virus informático, de la mano de Fred Cohen.

Mientras los primeros virus suponían simplemente un reto para sus diseñadores, que se jactaban de haber vulnerado los sistemas a los que pretendían infectar, el tiempo, la generalización de Internet, el uso de ésta como plataforma de negocio y en definitiva, el hecho de que de una manera u otra todos los ordenadores del mundo estén conectados entre sí, ha propiciado una escalada de códigos maliciosos, cada vez más destructivos capaces de generar pérdidas económicas millonarias, vulnerar los sistemas de seguridad de un país, e incluso llegando a acuñarse el término de cíber terrorismo, para definir determinados ataques a sistemas de información.

Por suerte, como decíamos al principio, los sistemas informáticos escolares no tienen que ver con el mundo empresarial, que es el más afectado por las vulneraciones de la seguridad informática, ni con sistemas sensibles, como los de defensa, interior o sanidad.

Nuestro problema se reduce considerablemente a mantener equipos en funcionamiento, listos para el uso y acceso a Internet, controlando los lugares a los que accede el alumnado.

Riesgos en la seguridad de los equipos informáticos

Aunque hoy en día es prácticamente imposible considerar a los equipos informáticos como entes aislados, si consideramos al ordenador como un elemento individual hay sólo tres elementos sobre los que tendremos que incidir para evitar agujeros de seguridad:

- Evitar accesos locales al equipo por parte de personas no deseadas.
- Evitar la contaminación del equipo por parte de elementos perniciosos que puedan dañar o ralentizar el funcionamiento del mismo, y que se aprovechan fundamentalmente de los sistemas de almacenamiento portátiles (llaves USB, tarjetas SD, discos duros portátiles) y/o de los sistemas de comunicación.
- Evitar agujeros de seguridad mediante el mantenimiento actualizado del equipo informático, su sistema operativo y los programas que utilicemos.

En cuanto a lo de evitar los accesos locales, la mayoría de los ataques se basan en nuestra ingenuidad a la hora de afrontar los problemas de seguridad. Es la llamada “Ingeniería social”.

Según Kevin Mitnik, uno de los “ingenieros sociales” más famosos de todos los tiempos, la obtención de información del usuario legítimo se basa en cuatro principios básicos:

1. Todos queremos ayudar.
2. El primer movimiento es siempre de confianza hacia el otro.
3. No nos gusta decir No.
4. A todos nos gusta que nos alaben.

Mediante este sistema es perfectamente posible obtener los datos de cualquier persona, incluso datos vitales para su economía.

Un ejemplo claro de la aplicación de este sistema es cuando se recibe una llamada al hogar desde un centro comercial conocido indicándonos que tienen una interesantísima oferta que ofrecernos. A lo largo de la conversación y tras habernos solicitado nuestro nombre, y nuestro DNI (según dicen, para comprobar nuestros datos), nos solicitan que para formalizar la oferta debemos darles el número de cuenta en la que cargar el gasto.

El fraude es completo, les hemos dado todos nuestros datos vitales incluidos los 20 dígitos de nuestra cuenta bancaria a una persona a la que no hemos visto siquiera la cara.

En las corporaciones empresariales es frecuente que alguien nos solicite en un momento determinado nuestro usuario y contraseña de acceso, haciéndose pasar por miembro del equipo de soporte informático y con el supuesto fin de acceder a determinadas tareas de reparación y mantenimiento de la máquina.

También es frecuente encontrarnos con usuarios que ante la incomodidad de cambiar las contraseñas y/o recordarlas las dejan escritas en un post-it adherido a la pantalla o con aquellas personas que utilizan como contraseña cosas sencillas como 1234, o el nombre de alguno de sus hijos.

Este tipo de vulneración de la seguridad tiene su correspondencia en el mundo de Internet con el llamado Phishing, del que hablaremos un poco más adelante.

La segunda de las posibles vulneraciones de seguridad se basa en la capacidad de los sistemas extraíbles de ser contaminados mediante virus que se auto replican no sólo en la dirección del ordenador contaminado hacia el elemento extraíble (llave USB, por ejemplo), sino desde éstos hacia los siguientes ordenadores.

Todos los dispositivos de almacenamiento extraíble tienen la capacidad de ejecutar de manera autónoma pequeñas aplicaciones. Esta facilidad que en sus orígenes se implementó para que al ser detectados por los sistemas operativos se lanzasen páginas de introducción a los contenidos, o logos representativos de su contenido que facilitasen la vida al usuario inexperto, se convierten al mismo tiempo en una herramienta al servicio de los diseñadores de virus que en último término buscan controlar nuestro equipo o dejarlo en estado no operativo.

La tercera de las posibles vulneraciones de los sistemas viene derivada de los llamados “agujeros de seguridad”.

El mundo de la informática avanza de una manera tan vertiginosa que los productos resultantes se comercializan sin haberse probado su fiabilidad al 100% en todas las

ocasiones y circunstancias posibles. Esto provoca que ante determinadas circunstancias, un mal funcionamiento de un programa, de un sistema operativo o del navegador correspondiente, hace que el sistema se bloquee facilitando que el intruso pueda acceder a nuestros datos, al contenido de nuestro disco duro o a la instalación de sus propios programas en nuestro equipo.

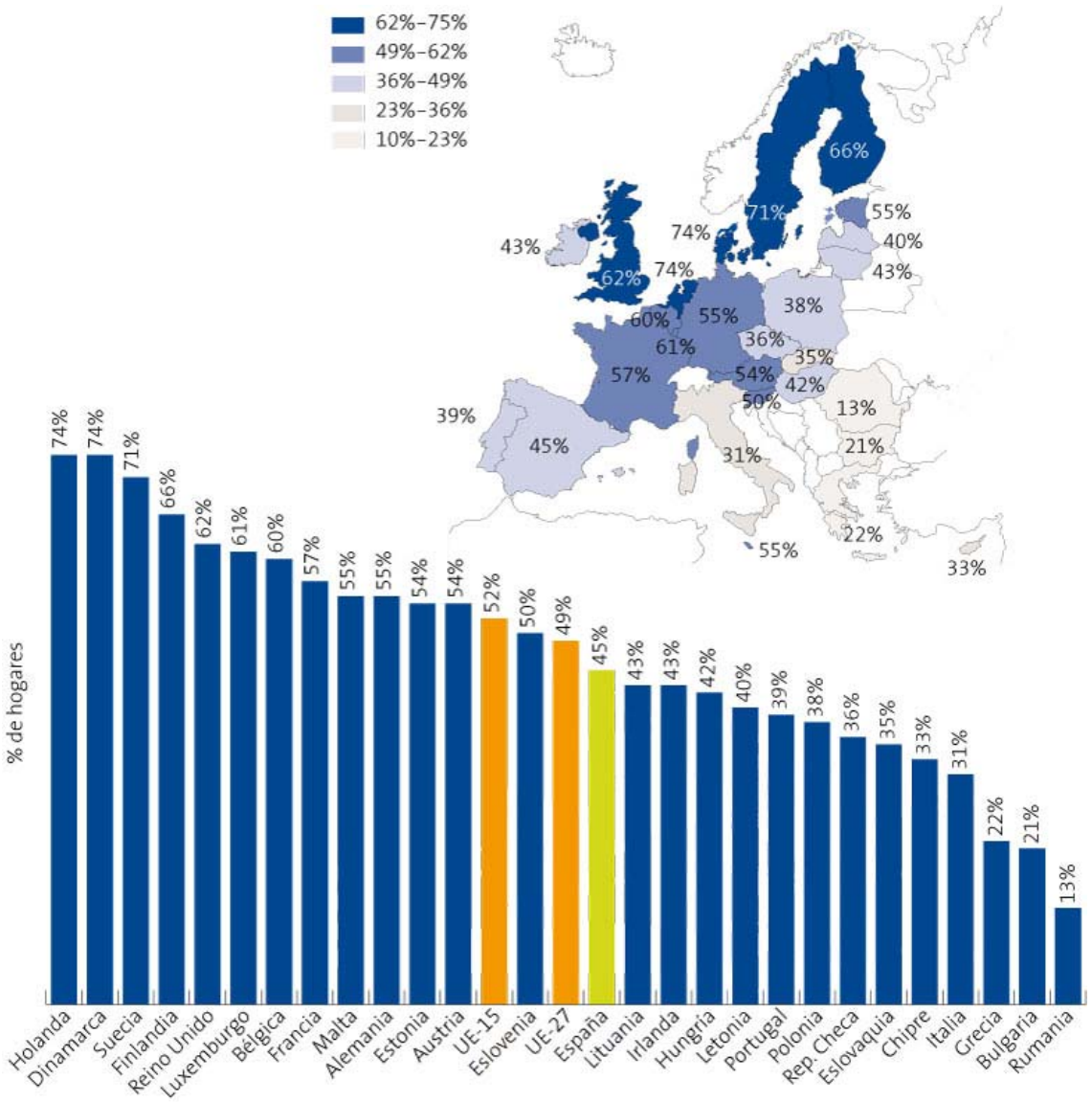
El submundo del fraude está en búsqueda permanente de estos agujeros para aprovechar las vulneraciones y controlar así los equipos informáticos, convirtiéndoles en auténticos zombies al servicio de la ilegalidad y sin conocimiento del usuario legítimo.

Las empresas desarrolladoras de los sistemas operativos y del software publican de manera permanente parches que corrigen los defectos encontrados. Es evidente que es necesaria una permanente actualización de los sistemas informáticos. Cuanto más actualizado, menos riesgo de vulnerabilidad.

Riesgos de la navegación por Internet

Como decíamos al principio, no se conciben hoy en día los equipos informáticos como entes aislados, sino integrados en redes que a su vez están todas conectadas entre sí.

Es más, si bien el acceso a Internet se hacía antes fundamentalmente vía modem, mediante líneas RTB o RDSI, actualmente, la mayoría de las conexiones se realizan mediante sistemas de conectividad de banda ancha, fundamentalmente ADSL, que permanecen operativas de manera continuada en el tiempo, es decir, no sólo duran lo que lo hace la llamada, sino que están permanentemente abiertas en tanto en cuenta el router de conexión esté enchufado a la red eléctrica y a la línea telefónica.



Los riesgos a la seguridad en los sistemas informáticos conectados a Internet se pueden clasificar según el objeto del ataque:

- Robo de identidad
- Virus, gusanos y troyanos
- Spyware
- Hackers y crackers
- Phishing y estafas on line
- Spam
- Contenidos Web inapropiados

Los riesgos listados no tienen por qué aparecer de manera aislada, sino que en la mayoría de las ocasiones actúan interrelacionados, de manera conjunta.

Hagamos una breve descripción de cada una de las amenazas.

El robo de identidad

El robo de identidad en Internet tiene siempre un fin ilícito y puede actuar en la búsqueda de diversos objetivos.

Desde su perspectiva más inocua, busca conocer los patrones de navegación del internauta con el fin de conocer sus gustos e intereses y con ello generar respuestas publicitarias con las que invadir al usuario en la búsqueda de que se pueda hacer negocio con él. La tecnología que subyace preferentemente es el uso de cookies, pequeños archivos en los que el navegador almacena información del usuario para guardarlo de una sesión a otra.

Cuando un usuario accede a una página de Internet, ésta deja una cookie en su sistema que empieza a llenarse con la huella de su actividad (por dónde ha navegado, que datos ha proporcionado a la red, etc.). Cuando se vuelve a navegar nuevamente por la página, se recoge la información de la cookie.

No todas las cookies son maliciosas. Algunos sitios Web precisan de ellas para poder ofrecer sus servicios al usuario.

La relación de usuarios y sus preferencias de navegación constituyen en sí mismo un negocio lucrativo pues se venden a empresas dedicadas a la publicidad.

Desde una perspectiva algo más agresiva, lo que se busca directamente es capturar los datos de identificación del usuario para posteriormente operar en su nombre en acciones ilegales, o directamente, sustraerle su identidad (login, clave de acceso) con el fin de directamente proceder a robarle en su banca electrónica o realizar compras por Internet y cargárselas a su cuenta bancaria.

Virus, gusanos y troyanos

Los virus informáticos tienen dos fines básicos. Por un lado, infectar cuantos más equipos y más rápido, mejor y por otro lado, provocar la pérdida de información, ralentización e incluso el deterioro de la máquina hasta dejarla no operativa.

Si bien los primeros virus informáticos entraban más en la categoría de reto para sus diseñadores, con consecuencias prácticamente inocuas, hoy en día suponen el origen de pérdidas económicas importantísimas a nivel mundial.

Si bien no hay estadísticas fiables al respecto, la consultora americana especializada Computer Economics cifra las pérdidas derivadas del malware (virus, troyanos, gusanos, etc.) en cerca de 92.000 millones de euros en los últimos 10 años, con base en los costes derivados de la pérdida directa de información, las paradas de sistemas y de las cantidades invertidas en la limpieza de los sistemas informáticos.

Los virus modifican el sistema operativo o los programas, que se infectan a medida que se ejecutan en el sistema, camuflándose de diferentes maneras.

A diferencia de éstos, los gusanos se replican a sí mismos en una espiral de crecimiento infinito que amplía los procesos ejecutados en la memoria de los sistemas. Una

característica específica de éstos es que el sistema se va ralentizando poco a poco hasta ser casi imposible su adecuado manejo.

Los troyanos no se comportan como un virus, sino que al igual que el caballo de Troya de la mitología griega, abre puertas para que los hackers puedan controlar nuestro equipo informático sin nuestro consentimiento, con dos fines básicos: conocer todo lo que hacemos para robarnos nuestras credenciales e identidad, y/o operar directamente desde él para realizar operaciones fraudulentas sin nuestro conocimiento.

La infección de troyanos suele venir acompañada de la instalación de programas aparentemente inocuos que se descargan gratuitamente desde Internet, o mediante acciones asociadas a un correo electrónico y página Web en la que el usuario lo activa sin querer al hacer clic en un determinado enlace o botón.

Spyware

El spyware es un pequeño programa que se introduce en el ordenador normalmente por un virus o un troyano y que se dedica a recopilar la información que el usuario contenga en su equipo y la procedente de su experiencia de navegación por Internet, intentando capturar identificaciones de usuarios y contraseñas, así como otros datos, ya explicados en el apartado robo de identidad. El troyano envía estos datos a través de Internet al ordenador del pirata informático, que recibirá todos los datos sin necesidad de moverse de su sitio.

El sistema de spyware también es utilizado en ocasiones para la vigilancia de los empleados en las grandes corporaciones con el fin de comprobar si sus actividades con el ordenador de la empresa se adecúan a las normas establecidas en la correspondiente corporación.

Hackers y crackers

Los hackers y los crackers son los individuos que están detrás de los procesos de vulneración de la seguridad que estamos describiendo.

Los hackers se dedican a la búsqueda de agujeros de seguridad con el fin de explotarlos para acceder a sistemas aparentemente securizados. A diferencia de los Crackers, que vulneran los sistemas para realizar acciones delictivas, los Hackers, al menos en su origen, buscan más bien el prestigio personal de ser capaces de encontrar la manera de entrar en sistemas altamente protegidos.

Phishing y estafas on line

La variedad de métodos para realizar fraudes en línea, es tan amplia que sería imposible describirla brevemente.

El phishing está íntimamente relacionado con la ingeniería social de la que hablábamos algunos apartados anteriormente. Lo que se busca es que sea el propio usuario el que proporcione sus datos de acceso y contraseña a determinados servicios, normalmente de tipo bancario, con el fin de proceder posteriormente a suplantar su identidad para hacer operaciones bancarias no autorizadas con sus cuentas.

Suele comenzar con un correo electrónico en el que argumentando problemas de seguridad u operaciones de mantenimiento del banco se nos solicita que volvamos a confirmar nuestros datos de acceso y contraseña en una página que suplanta la identidad de nuestra entidad bancaria, con lo que el robo de credenciales queda efectuado.

Un método ligeramente más sofisticado combina acciones de troyanos sobre nuestro fichero de Hosts, para llevarnos sin ser conscientes de ello a una página Web que imita perfectamente la apariencia de la portada de nuestra entidad bancaria en la que al querer entrar, sin ser conscientes de ello, proporcionamos nuestros datos de acceso a los piratas informáticos.

La estructura de navegación por Internet se basa en la jerarquía de servidores de nombres, lo que permite que al ingresar una dirección determinada, el equipo sepa exactamente a qué equipo tiene que dirigirse para proporcionarnos la página Web solicitada. Esta jerarquía comienza en un archivo del propio sistema operativo de la máquina llamado Hosts, que normalmente contiene una única línea con el dato "127.0.0.1 localhost". Esto significa que si introducimos la dirección "localhost" en el navegador, éste intentará recuperar la respuesta de nuestro propio equipo.

Si mediante algún troyano o virus alguien modificara nuestro archivo hosts, podría incluir direcciones web que suplantasen a las originales, por ejemplo, haciendo apuntar a la dirección de nuestro banco a otro ordenador diferente al mismo. Como consecuencia, nosotros, intentando acudir a nuestro banco entraríamos sin darnos cuenta en el ordenador de un pirata informático que procedería a robarnos limpiamente nuestra identidad.

Spam

El Spam, también llamado correo basura, es como su nombre indica, correo no deseado que recibimos en nuestro buzón.

La finalidad es doble: Por un lado, tiene un objeto meramente publicitario. Es como el buzoneo del mundo real, en el que nos depositan cantidades ingentes de papel de propaganda en nuestro buzón, pero en el mundo virtual. Normalmente va asociado a la información que sobre nuestra experiencia de navegación se ha obtenido por alguno de los medios descritos anteriormente, de manera que la publicidad que recibamos sea inicialmente de nuestro interés, aunque no siempre es así. Actualmente está muy extendido el Spam referido a la venta de medicamentos, viagra sobre todo.

Por otro lado, los correos de Spam suelen ser fuente de entrada de virus, troyanos, e intentos de phishing, por lo que hay que tener especial cuidado con ellos.

Contenidos Web inapropiados

Constituye uno de los mayores problemas con los que nos podemos encontrar en el mundo escolar, y de acceso a Internet en el hogar de nuestros niños y jóvenes.

El redireccionamiento de páginas Web o la aparición espontánea de ventanas (pop-ups) que nos conducen directamente a contenidos relacionados con el sexo o el juego, desde

páginas aparentemente inocuas es uno de los problemas más extendidos en la experiencia de navegación por Internet actualmente.

Pero no solamente se focaliza el problema en este aspecto automatizado en el que parece que los contenidos aparecen solos sin nuestro consentimiento, sino que forma parte del componente puramente educativo que como actuales y futuros internautas responsables debemos trabajar con los niños y jóvenes para evitar que accedan a contenidos de sexo, violentos, de apuestas, o perjudiciales para la salud, como por ejemplo los sitios que fomentan la anorexia.

Sistemas de protección

Ya hemos descrito el contexto y los posibles riesgos a la hora de enfrentarnos al problema de la seguridad informática y a la navegación por Internet.

Identificados los problemas potenciales vamos a ahora a centrarnos en intentar ver las posibles soluciones a los problemas planteados, que aun siendo seguramente por casi todos conocidas, no terminan de aplicarse plenamente ni siquiera en los entornos empresariales más rigurosos, cuanto menos en el ámbito de la escuela y del hogar.

Sistemas de protección local

Desde el punto de vista de la protección de nuestro ordenador, en su perspectiva local hay tres aspectos básicos a tener en cuenta, fáciles de implementar y que mejorarán sustancialmente nuestra experiencia de seguridad:

1.- Mantener actualizado el sistema operativo y el software instalado.

Es fundamental, para evitar posibles agujeros de seguridad en los sistemas derivados de las vulnerabilidades explicadas anteriormente, que mantengamos permanentemente actualizado nuestro sistema y el software instalado. Para ello, en la actualidad, los sistemas de actualización automática de los sistemas operativos nos facilitan enormemente la labor, al detectar de manera autónoma la configuración de nuestros sistemas y la necesidad de actualización, al igual que ocurre con la mayoría de los programas instalados.

2.- Cambiar periódicamente la contraseña de acceso al sistema.

Sea por el método que sea, si un usuario consigue las claves de acceso a un sistema, tendrá vía libre para operar con él sin nuestro consentimiento.

Para minimizar los riesgos derivados se debe cambiar con frecuencia la clave de acceso al sistema, utilizando para su configuración al menos una longitud de 6 caracteres alfanuméricos en los que combinar mayúsculas y minúsculas, letras, números y símbolos del tipo %, & o $.

Evidentemente hay que evitar palabras con significado común y relacionado con nuestro entorno próximo y no dejarlas al alcance de cualquiera en las proximidades del ordenador.

Como hoy en día es habitual tener múltiples usuarios y contraseñas para acceso no sólo al equipo local sino a múltiples sitios Web, existen programas que nos ayudan a recordárnoslas y las almacenan encriptadas. Uno de los mejores es Norton Password Manager, aunque existen multitud de sistemas que hacen lo mismo.

En la actualidad, las tarjetas criptográficas, y sobre todo la extensión del uso del DNI electrónico, permiten el almacenamiento de los certificados digitales necesarios para la identificación en la mayoría de los sitios de Internet (banca electrónica, servicios de la administración, etc.), aumentando con ello los niveles de seguridad y de privacidad que se pueden aplicar a los equipos informáticos y a la navegación por Internet.

3.- Instalar y mantener actualizado un programa antivirus.

Los programas antivirus monitorizan de manera permanente el sistema en busca de software malicioso en ejecución o en estado latente, con el fin de identificarlo, dar la alarma y si fuera posible desinfectar el equipo o al menos aislar el virus.

Existen múltiples sistemas antivirus de diferentes empresas y algunas soluciones gratuitas aunque es difícil establecer cuál de todas ellas es la mejor puesto que las comparativas realizadas por revistas especializadas usan unos parámetros muy diversos de evaluación y no exentos de influencias de las compañías explotadoras de las soluciones.

El Ministerio de Industria, Turismo y Comercio de España cuenta con un organismo autónomo dedicado a la seguridad informática denominado INTECO (Instituto Nacional de Tecnologías de la Comunicación) accesible a través de la dirección www.inteco.es que ofrece ayuda y consejos sobre soluciones de seguridad y antivirus de manera gratuita.

Sistemas de protección perimetral y navegación segura

Como su nombre indica, los sistemas de protección perimetral se colocan en el perímetro de las redes de comunicaciones, o más exactamente en los nodos de comunicación. Suelen estar formados por sistemas de filtrado de contenidos y sistemas de cortafuegos, también llamados Firewall. Podríamos incluir en este grupo también a las soluciones de cortafuegos de los equipos locales, que monitorizan todo el tráfico que sale y entra por la tarjeta de red.

Los sistemas cortafuegos se basan en listas de control de acceso en las que se definen direcciones y/o programas a los que se permite el acceso a Internet (listas blancas) o se les deniega el acceso (listas negras).

Los sistemas de filtrado analizan el contenido que circula por la red comparándolo con patrones previamente definidos en la búsqueda de virus, spam, o simplemente contenido no recomendable.

Existen muchas tecnologías aplicadas a los filtros, siendo actualmente los más usados en el filtrado de contenidos los de tipo semántico (búsqueda de cadenas de texto) y los de categorías, basadas en listas clasificadas de sitios Web en función de sus propios contenidos. Estas clasificaciones suelen realizarlas empresas o instituciones

supranacionales sin ánimo de lucro que se apoyan también en la experiencia de usuario para determinar cuáles son las Web recomendables y a cuáles se debe prohibir el acceso. Naturalmente, siempre hay un administrador del sistema que tiene la última palabra en cuanto a la configuración y nivel de profundidad de los análisis efectuados.

Sistemas de control parental

Basados en los sistemas de filtrado descritos en el apartado anterior son sistemas, bien locales, bien servicios en red ofrecidos por las operadoras para garantizar una experiencia segura de navegación por parte de los niños y los jóvenes.

Los mismos navegadores de Internet (Internet Explorer, Firefox, Safari, etc.) disponen de su propio sistema de control parental.

Tal y como vimos al principio, los ordenadores se conectan entre sí conformando redes y éstas a su vez se unen entre sí aportando conectividad entre ellas.

En cada red hay al menos un punto de comunicación con el exterior, por el que se accede a Internet. Los filtros de control parental se intercalan en estos puntos, de manera que todos los paquetes de información que atraviesan esos puntos son capturados, analizados conforme a patrones y bloqueados en el caso de que se encuentre que contienen información no deseada, según las definiciones que hayan marcado los administradores o responsables de los sistemas.

El problema surge con el nivel de profundidad de los controles. Si se basa en listas blancas y negras, y autorizamos el acceso a una determinada dirección de Internet, podremos encontrarnos con accesos cortados en niveles secundarios que podrían ser interesantes de visitar y que muy probablemente serán accedidos desde saltos a otros lugares diferentes al que se autorizó inicialmente.

Un nivel muy restrictivo de control parental, por tanto, puede hacer muy indeseable o incómoda la experiencia de navegación.

Por el contrario, y de manera análoga, una configuración muy permisiva hará ineficaz el filtro. Dónde colocar el punto de equilibrio dependerá en gran medida de la experimentación con el sistema que tengamos implantado.

Sociología de la seguridad

Hasta ahora hemos hablado fundamentalmente de problemas de seguridad y de mecanismos de protección que afectan fundamentalmente a los sistemas.

Pero como vimos al principio, salvo los equipos de los centros educativos que se destinen a tareas administrativas y con el fin de proteger los datos del alumnado en ellos contenidos, y a los que habrá que aplicar sistemas de encriptación y seguridad en los accesos, en el resto del equipamiento, el destinado a tareas docentes, lo vital es tenerlos operativos.

Teniendo en cuenta que normalmente, en un centro educativo, todos los equipos comparten la misma conexión a Internet, podremos plantear una primera barrera

mediante la configuración de las llamadas Vlanes (redes virtuales) independientes para la parte administrativa y la docente.

En cuanto a conseguir que los equipos del alumnado se mantenga operativo el mayor tiempo posible, podremos configurarlos para la recuperación rápida aplicando métodos de particionamiento de los discos duros y utilizando aplicaciones de restauración rápida e incluso métodos de arranque mediante sistemas on'live.

Entonces, ¿dónde está el problema?

Si bien es relativamente fácil el control de la experiencia de Internet en el aula, gracias al uso de los filtros de contenido descritos anteriormente, hoy, y sobre todo en los hogares, el uso de Internet se ha desplazado desde la simple navegación en forma de búsqueda de información, acceso a contenidos y juegos en línea hacia el uso de las redes sociales: facebook, tuenti, myspace, xing, etc.

De todas ellas, la más usada por los adolescentes es tuenti, con cerca de 150.000 perfiles registrados y con un experiencia media diaria de una hora y diez minutos de conexión.

Las redes sociales tienen la ventaja de unir virtualmente personas con intereses comunes. En ellas se contacta con los amigos, se comparten fotografías, canciones, videos, etc. De una manera absolutamente sencilla.

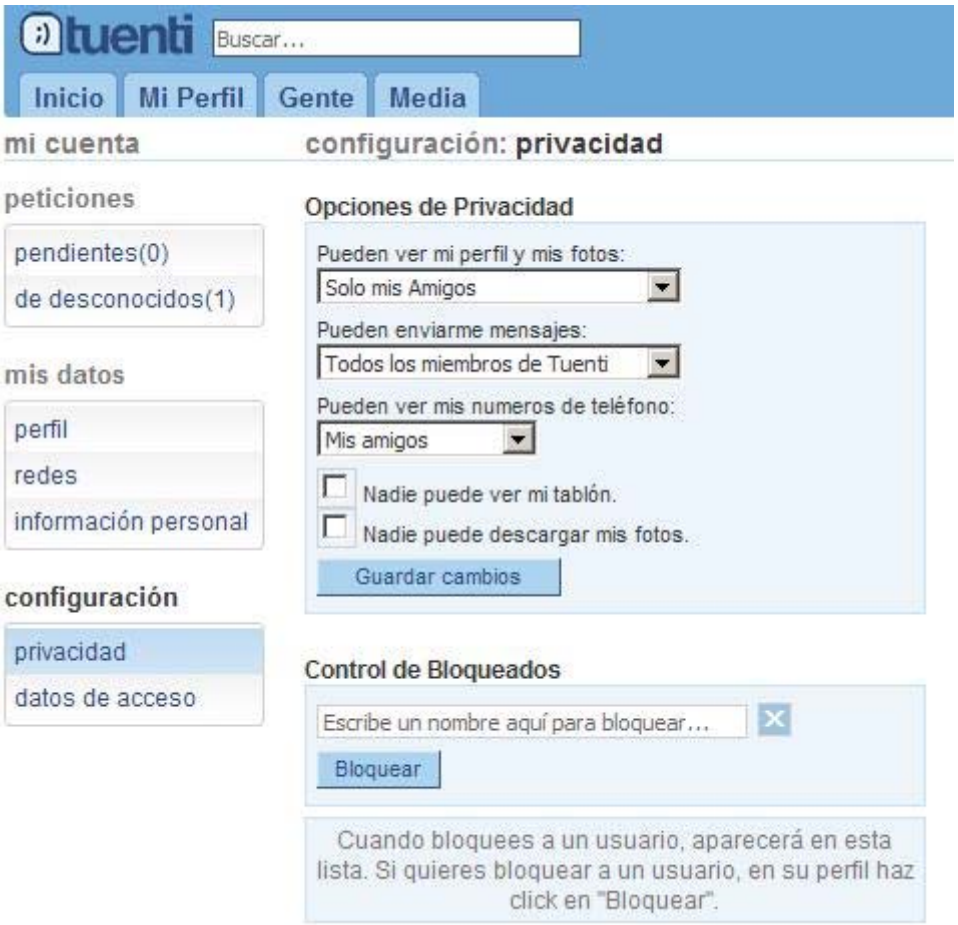
Los usuarios se registran gratuitamente en las diferentes plataformas confiados en que se están sumando a entornos seguros y que respetan su privacidad, invitando posteriormente a sus propios amigos que a su vez son incluidos, en una relación transitiva sin fin (los amigos de mis amigos son mis amigos).

Esto provoca que en un breve lapso de tiempo, como si de una estafa de modelo piramidal se tratase, las redes de "amigos" crecen de manera imparable y todos ellos tienen acceso a nuestros datos, y a nuestra imagen. Aun cuando a muchos de esos amigos ni siguiera les hayamos visto la cara.

Evidentemente, se puede cambiar la configuración de nuestro perfil para restringir los accesos a determinados contenidos nuestros y restringirlos a nuestros círculos más cercanos, pero no es la opción por defecto, siendo necesaria una navegación con al menos dos saltos para llegar a la página de configuración de nuestro perfil.

Adicionalmente hay que tener en cuenta que alojamos la información en ordenadores de los que somos usuarios pero que no controlamos nosotros, por lo cabe plantearse la cuestión de ¿qué ocurre cuando nos damos de baja en el servicio? ¿desaparecen nuestras imágenes y nuestros datos del mismo con nuestra baja?

La respuesta es No, o al menos no de manera inmediata. Según diversos estudios, aun habiéndose dado de baja un perfil en la red social a la que se pertenece se pueden encontrar fácilmente las imágenes allí colgadas hasta más de un mes después de producirse la baja. Y en este retraso, la estrella de las redes sociales es Facebook, que es una de las más populares y cuenta con más de 40 billones de imágenes almacenadas y con un crecimiento aproximado de 20 millones diarios (www.imatica.org).



Hay que tener en cuenta además que los usuarios tienden a colgar en la red imágenes, expresiones y datos que no publicarían en su vida diaria, pues la sensación que perciben es la de semi-anonimato.

Nada más lejos de la realidad. La red puede presumir de todo menos de garantizar el anonimato, pues deja rastro de absolutamente todo en todos y cada uno de los lugares por los que pasa.

Existen trucos y aplicaciones para ver las imágenes privadas de redes sociales, basta con hacer una búsqueda en google del tipo “trucos para ver imágenes privadas en facebook” y recibiremos como respuesta 14600 páginas de respuesta ofreciendo soluciones para poder hacerlo. Aun considerando que muchas no funcionen realmente y otorgándole un margen de fiabilidad del 1% a la información, habremos recibido al menos 146 páginas con una solución correcta, que curiosamente aparecerán entre los primeros puestos del ranking de respuesta. En el caso de redes sociales más usadas por los menores, el número de respuestas ante una búsqueda de ese tipo es sensiblemente menor, pero significativo (1800 respuestas, al menos 18 válidas siguiendo el criterio restrictivo).

Adicionalmente al problema de la privacidad y de la ampliación progresiva de la red de “amigos”, existe el de la suplantación de la personalidad. Nadie nos garantiza que el que está al otro lado del Chat y/o de los mensajes es quien dice ser, por mucho que se haya presentado como un niño o niña de nuestra edad.

Aunque el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal establece que sólo se pueden recabar datos de menores con el consentimiento expreso de sus padres y sin relacionarlos con el resto de los datos correspondientes a la unidad familiar, y que es el responsable del fichero informático el que debe garantizar no sólo la custodia y fidelidad de los datos, sino la veracidad de las autorizaciones otorgadas, la realidad de Internet hace que sea compleja su efectiva aplicación, pues los sistemas que albergan a las redes sociales tienen un carácter supranacional, con legislaciones diferentes para cada país y con una valoración diferente en los mismos del grado de protección que se debe dar a la infancia.

La consecuencia de esto es que es difícil evitar que algún adulto se haga pasar por niño con el fin de establecer contactos y relaciones e iniciar un proceso de Grooming (acoso sexual desde un adulto a un menor en la red).

Y no sólo el acoso desde el punto de vista del adulto al menor, sino el acoso entre iguales (ciberbullying), por ejemplo, haciendo públicas es redes sociales imágenes no autorizadas sobre compañeros o compañeras de clase en situaciones comprometidas, con componente violento o de vejación del individuo.

Por último, no deberíamos olvidar el problema derivado de la posible adicción a Internet, con especial hincapié en el caso de los menores, pudiendo llevar aparejado trastornos en el comportamiento de los mismos e incluso percepciones incorrectas de la realidad, y que en estadios graves deben ser abordadas desde el punto de vista del tratamiento médico psiquiátrico o psicológico.

Consejos para minimizar los riesgos en la navegación por Internet.

Finalmente, y a pesar de los riesgos apuntados en la presente ponencia, la experiencia de navegación por Internet no tiene por qué ser negativa.

El mundo de la informática y el acceso a Internet nos ofrece un horizonte de posibilidades de éxito para la educación, el trabajo, la ampliación de la relación social y el ocio, siempre que se guarden unos mínimos consejos básicos, no muy difíciles de implementar y que encontramos como recomendación en todas las instituciones, tanto públicas como privadas que se dedican a analizar, perseguir y corregir los comportamientos anómalos e ilícitos que también se producen en la red de redes.

Consejos para la protección del equipo

1. Mantente informado sobre las novedades y alertas de seguridad.
2. Mantén actualizado tu equipo, tanto el Sistema Operativo como cualquier aplicación que tengas instalada.
3. Haz copias de seguridad con cierta frecuencia, para evitar la pérdida de datos importante.
4. Utiliza software legal que suele ofrecer garantía y soporte.
5. Utiliza contraseñas fuertes en todos los servicios, para dificultar la suplantación de tu usuario (evita nombres, fechas, datos conocidos o deducibles, etc.).

6. Utiliza herramientas de seguridad que te ayudan a proteger / reparar tu equipo frente a las amenazas de la Red.
7. Crea diferentes usuarios, cada uno de ellos con los permisos mínimos necesarios para poder realizar las acciones permitidas.

Consejos para una navegación segura.

1. Para evitar virus, descarga los ficheros solo de fuentes confiables.
2. Descarga los programas desde las páginas oficiales para evitar suplantaciones.
3. Analiza con un antivirus todo lo que descargues antes de ejecutarlo.
4. Mantén actualizado el navegador para protegerlo contra los últimos ataques.
5. Como apoyo para saber si una página es confiable utiliza analizadores de URLs.
6. Configura tu navegador para que sea seguro.
7. Ten precaución con las contraseñas que guardas en el navegador, y utiliza siempre una contraseña maestra.

Consejos para el uso seguro del correo electrónico.

1. Desconfía de los correos de remitentes desconocidos, ante la duda elimínalo.
2. No abras ficheros adjuntos sospechosos procedentes de desconocidos o que no hayas solicitado.
3. Utiliza el filtro anti-spam y marca los correos no deseados como correo basura.
4. Ten precaución con el mecanismo de recuperar contraseña, utiliza una pregunta que sólo tu sepas responder.
5. Analiza los adjuntos con un antivirus antes de ejecutarlos en tu sistema.
6. Desactiva la vista previa y la visualización en HTML de tu cliente de correo para evitar el posible código malicioso que pueda estar incluido en el cuerpo de los mensajes.
7. No facilites tu cuenta de correo a desconocidos ni la publiques *'alegremente'*.
8. No respondas a mensajes falsos, ni a cadenas de correos para evitar que tu dirección se difunda.
9. Cuando reenvíes mensajes a múltiples destinatarios utiliza la copia carbón oculta –CCO o BCC- para introducir las direcciones

Consejos para las transacciones económicas seguras por Internet

1. Observa que la dirección comienza por https que indica que se trata de una conexión segura porque la información viaja cifrada.
2. Asegúrate de la legitimidad de la página; con la barra de navegación en verde total confianza, con la barra en azul debemos conocer previamente que esa página coincide con la entidad solicitada.
3. Ten en cuenta que tu banco NUNCA se pondrá en contacto contigo para pedirte información confidencial.
4. Evita el uso de equipos públicos (cibercafés, estaciones o aeropuertos, etc.) para realizar transacciones comerciales.

5. Desactiva la opción ’autocompletar’ del navegador si accedes desde un equipo distinto al habitual o compartes tu equipo con otras personas.
6. Cierra tu sesión cuando acabes, para evitar que alguien pueda suplantarte.
7. Configura tu navegador para que puedas realizar cualquier transacción económica de forma segura.

Consejos para la participación segura en redes sociales

1. Lee las políticas de uso y privacidad de los diferentes servicios antes de utilizarlos, sobre todo lo relacionado con la política de privacidad y la propiedad última de los que se publica en la red social.
2. Piensa antes de publicar, no sea que luego te arrepientas.
3. Valora que información deseas revelar y controla quién puede acceder a ella.
4. Controla tu lista de contactos, y antes de agregar a alguien tomate tu tiempo para asegurarte de su confianza.
5. Las redes sociales contienen las mismas aplicaciones que utilizan los atacantes para propagar los virus –correo, mensajería, navegación, etc.-, mantén las mismas recomendaciones.
6. Utiliza contraseñas seguras para que no te suplanten.
7. Si crees que estás siendo víctima de acoso contacta inmediatamente con el servicio de atención exponiéndole tu caso.

Consejos específicos para la experiencia segura de los menores en Internet

1. Educa al menor sobre los posibles peligros que puede encontrar en la red.
2. Acompaña al menor en la navegación cuando sea posible, sin invadir su intimidad.
3. Advierte al menor de los problemas de facilitar información personal (nombre, dirección, teléfono, contraseñas, fotografías, etc.) a través de cualquier canal.
4. Desaconséjale participar en charlas radicales (provocadoras, racistas, humillantes, extremistas, etc.) ya que pueden hacerle sentir incómodo.
5. Infórmale de que no todo lo que sale en Internet tiene que ser cierto, ya que pueden ser llevados a engaño con facilidad.
6. Indique claramente a su hijo que la comisión de delitos también se puede realizar a través de Internet y que el desconocimiento de la ley no exime de su cumplimiento. Acciones como la descarga ilegal de programas, películas, música, el acoso a compañeros, etc., están severamente penadas por la ley.
7. Presta atención a sus ’ciber-amistades’ en la misma medida que lo haces con sus amistades en la vida real.
8. Pídele que te informe de cualquier conducta o contacto que le resulte incómodo o sospechoso.
9. Vigila el tiempo de conexión del menor a Internet para evitar que desatienda otras actividades.
10. Crea una cuenta de usuario limitado para el acceso del menor al sistema.

Consejos sobre el acceso a Internet en el hogar

1. Coloque el ordenador o dispositivo de acceso a Internet en un lugar común. Podrá comprobar discretamente los lugares que visita su hijo/a.

2. Acompañe a su hijo/a en la experiencia de navegación por Internet, en la búsqueda de información y en el juego, procurando ser un partícipe más y no como elemento controlador. Cuanta más confianza tenga su hijo/o en Usted y más percepción de que se le respeta, más fácil le será contarle todo lo que hace.
3. Sobre todo, hable con su hijo/a. Una buena comunicación es el cauce perfecto para prevenir los riesgos y para ayudarle rápidamente en caso de apuro.

Enlaces de interés

www.inteco.es	Instituto Nacional de Tecnologías de la Comunicación del Ministerio de Industria, Turismo y Comercio de España.
www.osi.es	Oficina de Seguridad del Internauta del Ministerio de Industria, Turismo Comercio de España.
www.alertaenlinea.gov	Página de seguridad de la Comisión Federal de Comercio de los Estados Unidos de América.
www.fosi.org	Family Online Safety Institute, organización británica para la seguridad en Internet de los niños y las familias formada por un consorcio de empresas de las comunicaciones, el hardware, el software y la seguridad.
http://recursostic.educacion.es/observatorio	Observatorio tecnológico del Instituto de Tecnologías Educativas con abundante información sobre aplicaciones de seguridad informática, filtrado de contenidos y redes sociales.
http://www.ite.educacion.es/padres/videojuegos/menores_e_internet/	Página dedicada a los menores y el uso de Internet del Instituto de Tecnologías Educativas.
http://e-libros.fundacion.telefonica.com/sie09/	Informe sobre la sociedad de la información en España, en el año 2009 de Fundación Telefónica.

Licencia