# III SEMANA de SEGURIDAD INFORMÁTICA

Del 23 al 27 de Marzo de 2009

# BoleTIC

# 2009

# Editorial

*Por Fernando Ferrer Molina, Presidente de Fundación Dédalo*

Ya ha pasado un año desde la publicación del primer BoleTIC, que vió la luz en la 2ª Semana de Seguridad Informática celebrada en abril de 2008. El éxito local y nacional de la iniciativa fue indiscutible. Los asistentes a las jornadas programadas, además de la repercusión en medios y las entidades participantes, hablaron por sí solas.

En esta edición hemos trabajado en la misma línea, con la colaboración de profesionales de primer nivel en el mundo de las Tecnologías, organizando una amplia y variada programación de actividades para todos los públicos: **Talleres** sobre redes sociales para estudiantes de la ESO y alumnos de primaria en colaboración con Fundación CTIC, **Tutoriales** para ciudadanía, sin olvidarnos del sector empresarial y profesional, para los que se han organizado tres interesantes **Jornadas** impartidas por entidades de referencia como AENOR, Informática64 e INTECO. Sin duda, es un lujo contar en Tudela con ponentes de toda la geografía nacional, expertos en seguridad.

El evento central de la *III Semana de seguridad informática* es una **Mesa de debate**, cuyo objetivo es sensibilizar y hacer promoción sobre un uso seguro de las Nuevas Tecnologías. En este evento participan entidades con amplia experiencia y reconocido prestigio en materia de seguridad, ofreciendo un foro de encuentro y un espacio en el que los participantes pueden jugar un


papel protagonista aportando sugerencias, dudas e inquietudes.

Desde Fundación Dédalo tenemos el firme convencimiento de que construir un mundo digital más seguro es posible, con el esfuerzo, participación y apoyo de todos los estamentos, públicos y privados.

Para conseguir este objetivo debemos disponer de la información adecuada, tomando conciencia de la necesidad de actuar en el mundo digital de la misma forma que lo hacemos en el mundo real. Es necesario educar a toda la población, haciendo especial hincapié en el ámbito escolar, para fomentar un uso racional de las Tecnologías y aprovechen todo su potencial, midiendo adecuadamente los inconvenientes y peligros que puede ocasionar un mal uso de las herramientas informáticas.

Disfrutad de este BoleTIC, en el cual se recogen artículos elaborados en exclusiva para todos vosotr@s por personas con amplio bagaje y experiencia en el sector de las Nuevas Tecnologías.

## INDICE

# Formación para la e-inclusión integral de la comunidad educativa

***Por Paco Prieto,***

***Director de Sociedad de la Información de Fundación CTIC, Asturias***

Actualmente, los menores asumen con normalidad la presencia de las tecnologías en la sociedad, conviven con ellas y las introducen sin dificultad en su vida cotidiana.

Este aspecto ha de ser tenido en cuenta para propiciar una educación acorde con nuestro tiempo, introduciendo las herramientas necesarias e innovando con propuestas didácticas, que utilicen las tecnologías como un recurso que favorezca el trabajo en equipo, el desarrollo de las destrezas sociales, la creatividad, la posibilidad de experimentar y la curiosidad por conocer e investigar y siempre desde la perspectiva del uso responsable de las TIC.

La adquisición de las destrezas básicas para el uso responsable de Internet debe empezar en las etapas iniciales, mediante el fomento de una cultura de la prevención, puesto que las estadísticas nos demuestran que la población joven es quien hace un mayor uso de las tecnologías y con porcentajes bastante superiores al resto de tramos de edad. Así, el 90.3 % de la población española de 16 a 24 años y el 82,2% entre 10 a 15 años, es usuaria de Internet, según los últimos datos de la *Encuesta de Equipamiento y uso de las TIC en los Hogares del INE*, correspondientes a 2008

Se han dado pasos en ese sentido, hacia la integración curricular de las TIC en la enseñanza formal. De hecho, el tratamiento de la información y la competencia digital es una de las nueve competencias básicas que se desarrollan en todas las etapas de la enseñanza obligatoria.

Aún así, debemos ser conscientes de que la formación en el uso de las Tecnologías de la Información y la Comunicación dirigidas a menores no es suficiente, especialmente en lo relativo a la identificación y tratamiento de los riesgos y el uso responsable. Los jóvenes realizan muchos aprendizajes a través de canales informales, no estructurados, con una transmisión más operativa del cómo hacer determinadas operaciones con las Tecnologías de la Información y la Comunicación, y por lo tanto, desde la comunidad educativa no se puede garantizar que cuestiones relacionadas con la prevención y el Uso seguro de Internet, se interioricen por parte de los jóvenes cuando se acercan a las Tecnologías de la Información.

También hemos de darnos cuenta de que los distintos colectivos (madres y padres, profesorado y jóvenes) se acercan y viven las Tecnologías de la Información y la Comunicación de forma diferente. Para las personas que tienen menores bajo su responsabilidad la introducción de las TIC en sus vidas puede generar cierto rechazo y aumentar las preocupaciones. El conocimiento es, sin ninguna duda, la mejor receta para minimizarlas. Saber cómo realizar un uso seguro de Internet y de otras TIC, así como conocer los servicios de los que la ciudadanía dispone constituye un antídoto infalible para evitar riesgos innecesarios.

Por tanto, es preciso fomentar la formación tecno-pedagógica tanto del profesorado como del entorno familiar, para que madres, padres y educadores conozcan las potencialidades educativas de las TIC y puedan poner en marcha los mecanismos para evitar posibles riesgos.

En otras palabras, debemos trabajar por la e-inclusión integral de la comunidad educativa (padres y madres, profesorado), además de los y las menores, en torno a un uso seguro y constructivo de Internet y las TIC. Por ello, conviene impulsar proyectos con perspectiva intergeneracional, para lograr reunir a toda la familia en torno a las Tecnologías de la Información y la Comunicación y estimular, así, desde la educación, acciones que aúnen didáctica y entretenimiento.

Más allá de planteamientos teóricos, desde la Fundación CTIC (www.fundacionctic.org), estamos trabajando con algunas iniciativas y propuestas de programas educativos que fomentan el uso seguro de las Tecnologías de la Información y la Comunicación entre diferentes colectivos destinatarios.


Voy a comenzar por el entorno en el que quizás exista más desconocimiento: la familia. En este frente, planteamos una **Escuela Tecnológica de Familias**. Apoyándonos en una producción audiovisual, hemos desarrollado materiales, para trabajar en talleres o "auto consumir", sobre diferentes temáticas que ayudarán a las madres y padres a incorporar las TIC en sus hogares, sin miedos ni complejos. A través de veinte audiovisuales y sus correspondientes fichas, esta colección *destripa* las tecnologías y sus servicios mostrando qué son y cómo se pueden utilizar sin riesgos.

En segundo lugar, los y las más *peques* de la casa. Nos dirigimos a un rango de edad entre tres y siete años, que sabemos que emplea el ordenador en sus rutinas de colegio y de familia, de manera totalmente normalizada. Por lo tanto, desde el principio, deben tener el conocimiento y la seguridad necesarios; nuestra pizpireta

e ingeniosa **Fantastic Nikä** se encarga de proporcionárselos. Se trata de una *muppet* que, bien desde la pantalla, bien desde las fichas y otros materiales didácticos que, desde este programa, hemos elaborado tanto para el público infantil, como para progenitores y docentes, con su ingenio y desparpajo sabe meterse en el bolsillo a su audiencia. Nikä resulta de aplicar un método innovador que fusiona la educación, la temática TIC, el medio audiovisual y las *muppets* o marionetas.

Por último, **Seguridad y Uso Responsable de las TIC**, colección audiovisual de veinte capítulos dirigidos a niños y niñas de ocho a doce años. Con creatividad, frescura, fuerza visual y la utilización de personajes de la "misma altura" que la audiencia destinataria (perspectiva de igual a igual), tiende el anzuelo a los chavales para que utilicen las TIC con responsabilidad y buen juicio. La protagonista, en este caso, es una adolescente real que desgrana las tecnologías y servicios con los que habitualmente conviven los y las preadolescentes: telefonía móvil, ordenadores, wi-fi, blogs, redes sociales, etc.

*Podéis ampliar información en la web de*
*Internet y familia, un proyecto integral de Fundación CTIC.*

***http://www.internetyfamilia.com/superportal/opencms***

## *LA ESPERANZA ES LO ULTIMO QUE DEBE PERDERSE*

***Por Luis Arroyo Galán***

***"Una fórmula para salir de esta crisis, podría ser al líder rogando y con internet dando"***

Es tal la cantidad de problemas económicos que nos llegan a través de los medios, algunos descritos con todo lujo de detalles, que a aquellas pocas personas que aun tenían ilusión por hacer algo (comprar, ahorrar, invertir, crear empleo…), se les habrán quitado las ganas con tanta zarabanda mediática.

Al decir de los expertos, estamos sufriendo tres tipos de crisis: financiera, económica y de confianza. Para las dos primeras, pocas son las recetas a nivel individual que podrían ponerse en marcha; es aquí donde los líderes deberían de dar el do de pecho, pero a tenor de los no-resultados que se están consiguiendo, parecería que nuestra clase dirigente se ha quedado afónica.

Los ciudadanos que confían en la llegada del maná de la recuperación caído del cielo, no se dan cuenta que esta lluvia les ha sido anunciada una y otra vez, pero cuando llega el momento pronosticado, se les dice que deben esperar a otro próximo mañana.

De las tres crisis enunciadas mas arriba, la desconfianza, al decir de los expertos, puede que sea la más peligrosa, por una doble razón; en primer lugar porque sin su resolución, no puede acabarse con las otras dos, y porque su final feliz depende del estado de ánimo de millones de personas.

Y aquí es donde entramos cada uno de nosotros, pero ¿Cómo es posible que una crisis que afecta a miles de millones de terrícolas, tenga que ser superada únicamente con las decisiones de solo unos pocos líderes?

Hasta aquí perfecto, pero ¿Cómo un ciudadano como yo, aislado en mi entorno personal, familiar y laboral, puedo hacer algo por la recuperación económica de la sociedad en la que vivo? Pues muy fácil, teniendo en cuenta que en España hay mas de veinte millones de cibernautas (mas de mil millones a nivel mundial) y que puedo estar conectado en red con todos y cada uno de ellos.

Si compramos y vendemos a través de Internet, si comercializamos nuestros productos mediante la red, si agilizamos nuestras relaciones con la e-administración, y si aprovechamos al máximo las posibilidades que nos ofrece la red de redes, habremos contribuido a potenciar un muy importante sector de la economía, y sin salir de casa.

Todos sabemos que el sustrato económico de nuestro país, no lo es otro que las PYMEs y micropymes. Muchos centenares de ellas (¿miles?) han conseguido **casos de éxito**, es decir, logros empresariales cuantificables (incrementos de plantilla, de ingresos, de número de clientes...) mediante el uso innovador de Internet.

Dentro de las actividades previstas para el **diadeinternet 2009**, figura la difusión de casos de éxito. Esta comunicación a la sociedad confiamos en que tenga las siguientes ventajas: pone cara y ojos a lo conseguido con el uso innovador de Internet, explica la forma en que se ha logrado, y contribuye a mejorar la confianza en el sistema economico.

Una fórmula para salir de esta crisis podría ser, al líder rogando y con Internet dando.

***Luis Arroyo Galán***
*Coordinador diadeinternet 2009*

## ¿Nuevos riesgos con las Redes Sociales?

Para empezar, conviene señalar que las Redes Sociales no son las culpables, como se tiende a apuntar, no en último extremo. Se trata simplemente de una evolución de Internet donde confluyen una serie de servicios que ya venían existiendo, como la mensajería instantánea y la edición de blogs (con Messenger y Fotolog a la cabeza). Cierto es que hay otras opciones nuevas de alto valor añadido y potencia, pero en esencia estamos hablando de datos personales, de contacto con otras personas y de edición de contenidos. Nada nuevo antes de las Redes Sociales. Internet no es sino una gran Red Social y éstas subconjuntos a medida de la misma.

Lo que sí es cierto es que, por su finalidad, estas plataformas invitan a la participación activa, esto es, a conocer otras personas (formando la Red), a "subir" contenidos (cada vez más audiovisuales) tanto propios como ajenos, que además van trazando los perfiles e intereses de cada cual. Y en demasiadas ocasiones priorizan "su negocio" frente al de sus usuarios, en especial, de los menores, buscando tener más datos para vender y cruzar, intensificando al extremo las opciones de "conectarse con otra persona" incluso de forma transparente para el usuario, imponiendo condiciones de uso abusivas, potenciando indiscriminadamente las afiliaciones automáticas para ganar impactos publicitarios por volumen de usuarios. Y en este punto habría que sacar a colación el "interés superior del menor" promovido por la Convención de los Derechos del Niño y la responsabilidad legislativa de las instituciones, junto con términos como Responsabilidad Social Corporativa que las entidades, con legítimo ánimo de lucro, sería deseable observaran…. Pero establecer los límites es un largo debate y volveríamos a usar la controvertida palabra "autorregulación".

Opino que la esencia de la Red es la misma que hace 15 meses, y los usuarios también. Y los problemas o riesgos para los menores, los mismos que acompañan a Internet desde el inicio. Sin embargo, la forma en que operan las redes sociales puede incrementar la incidencia de las situaciones de riesgo.

## ¿Cómo afectan las redes sociales a la seguridad de los menores?

Podemos decir que sí han intensificado las probabilidades de riesgo a tenor de las características que les son comunes a la mayoría:

- **Pérdida del criterio de referencia.** Promueven más las relaciones entre personas a través de otras personas, por lo que se pierde el control directo de la referencia y el criterio de selección o confianza usado se diluye según los nodos se distancian. Ampliar relaciones es en sí positivo, pero el efecto negativo es más probable cuando no se ha podido usar el propio criterio de filtrado, sino uno inducido, digamos "transitivo". *Ejemplo*: por cortesía o costumbre abro mi Red a cualquier amigo de un amigo que me lo pide… y resulta que me tengo que remontar 3 niveles para ver cómo entró en "mi red" y con ello el criterio de filtrado se ha desvirtuado varias veces.

- **Exceso de operatividad sin intervención directa y consciente del usuario.** Disponen de demasiadas funciones automáticas que el usuario novato desconoce. Ayudan a crecer a la Red, y en teoría a la función relacional de la misma buscada por los propios usuarios, pero también a potenciar la propia plataforma. *Ejemplo*: me doy de alta en la Red X y salvo que preste atención para impedirlo (si es que conozco que lo hace) serán invitados de manera automática a unirse a mi red (lo hagan o no ya saben, cuando menos, que yo me he dado de alta) todas las personas que tenía anotadas en mi servicio de webmail (tipo hotmail, gmail…) si es que las compañías respectivas llegaron a ese acuerdo al que yo les autoricé, seguro, aceptando sus condiciones generales que no llegué a leer.

- **Funciones demasiado potentes y de efectos desconocidos a priori**. Existen posibilidades en exceso avanzadas para compartir todo tipo de cosas. Estas "gracias" que el programa nos prepara pueden ser un grave problema, sobre todo para quien desconoce su funcionamiento. *Ejemplo*: si te etiquetan en una fotografía (cosa que tú desconocías se pudiera hacer) y tienes el perfil más o menos abierto, es como si la pusieras tú mismo a la vista de mucha gente. Significa esto que alguien ha decidido por

ti qué hacer público y, además, compartirlo, porque sale o no, contigo, en esa fotografía.

- **Concentran el universo de relaciones de manera intensiva.** De sobra es conocida la escasa perspectiva que tienen los menores de la repercusión y alcance de lo que publican (lo dice quien ha hablado con muchos cientos). Cualquier cosa en la Red puede tener un eco brutal. Si eso afecta directamente a "mi red", el efecto puede ser demoledor, como el de un veneno concentrado, selectivo. *Ejemplo*: una calumnia en una página web puede tener más o menos eco, pero si se vierte en el contexto de tu Red, el efecto es mucho más rápido y doloroso, aunque no lo pueda ver tanta gente.

- **Guardan, explícitamente o no, información muy precisa.** Basan las relaciones en el perfil, intereses y actividad de los usuarios por lo que les requieren muchos datos y les registran sus acciones dentro de la propia Red. El usuario es víctima de un rastreo intensivo (atención, como lo es en los videojuegos y otras muchas actividades online que requieren identificación previa) que adecuadamente tratado puede crear una información de mucho más valor que la explicitada. *Ejemplo*: desde que entro en la Red pueden quedar registrados mis movimientos e intereses de todo tipo más allá de la información del perfil que de forma voluntaria proporcioné (dónde pincho, con quién hablo, cuánto tiempo dedico…).

- **Presentan al usuario las opciones de manera demasiado interesada, lo que suele implicar pérdida de privacidad.** Tras una supuesta intención de ayudar y agilizar, suele ser política común de las plataformas de Redes Sociales ayudarse a sí mismas. Así, pondrán muy poco énfasis en que el usuario configure las opciones de privacidad de los datos y, sin embargo, insistirán en que completemos los perfiles con todo tipo de cuestiones. *Ejemplo*: al darme de alta me preguntan datos de lo más variado sin los que no me dejarían registrarme, tras lo cual podré empezar a utilizar la Red sin haber configurado de forma explícita con quién y qué tipo de datos personales o de actividad quiero compartir.

Creo que estos son los principales factores diferenciales en materia de uso seguro de Internet producidos por la irrupción de las Redes Sociales. No he querido abordar temas genéricos como el control de las edades, las medidas de seguridad, la supervisión de los datos y las comunicaciones… que, como digo, ya eran cosa de la Internet anterior a las Redes Sociales, donde ya se prodigaban efectos en forma de ciberbullying y grooming.

Por último, hay una cuestión a la que creo se alude con demasiada poca frecuencia y que me gustaría destacar acá por su transversalidad en lo que tiene que ver con la protección del menor en la Red. Es preciso elevar la cultura de lo que denomino "higiene del ordenador". Muchos problemas, en las redes o fuera de ellas, tienen su origen en el robo de datos o claves personales del mismo ordenador del usuario, que dan pie al comienzo de chantajes. *Ejemplo*: si tengo mi lista cerrada de contactos, digamos en el Messenger (para no volver sobre las redes sociales) y cuando mi amiga María deja de ser María para ser quien le ha robado su clave… estoy peor que frente a un desconocido.

***Jorge Flores Fernández***
***Director de PantallasAmigas***


*www.pantallasamigas.net "trabajando por un mundo más seguro"*

## ¿Es peligroso navegar por internet?

***Por Fernando de la Cuadra***

Hace 20 años, más o menos, cuando los fabricantes de antivirus empezaban a desarrollar sus productos, los usuarios eran muy pocos. Los ordenadores personales, que hoy en día los encontramos hasta en la sopa (literal, he visto sopa de "teclas de ordenador"), eran unos objetos muy raros en las empresas, y no hablemos de las casas. Quien tenía un ordenador era un bicho raro, y le sobraba el medio millón de pesetas (que son 3.000 euros, para los más jóvenes) para comprarse un aparato que servía para jugar y poco más.

Por aquel entonces desarrollar un antivirus era una tarea relativamente sencilla. Con tener vigilados a media docena de virus se consideraba que el usuario estaba protegido contra la mayor parte de las amenazas. Y no olvidemos que la propagación de virus era una cosa realmente lenta, ya que Internet no era más que una extraña red científica y militar a la que nadie soñaba conectarse desde casa.

Sin embargo, hoy en día cualquier persona que tenga interés y pueda hacer un pequeño esfuerzo económico puede comprarse un ordenador (he visto ofertas de hasta 250 euros por un portátil bastante decente) y conectarse a Internet enseguida. Esto supone un riesgo inmenso, ya que si hace 20 años había pocos virus de los que preocuparse, hoy en día los laboratorios de ESET están detectando decenas y cientos de miles de virus nuevos todos los días.

¿Puede un antivirus luchar contra eso? Evidentemente, pueda o no pueda, debe hacerlo. Las tecnologías han evolucionado tanto que es posible hacer un programa de seguridad que detecte millones de amenazas distintas sin que el usuario note que se está llevando a cabo esta tarea en el sistema.

Para ello hace falta una ingente tarea de investigación y desarrollo, una creatividad y una imaginación mucho más grande que la que llevan a cabo los desarrolladores de virus. Hay que estar un paso por delante de ellos, para saber qué nueva maldad van a planear y hasta dónde van a llegar.

Pero desgraciadamente, no siempre podemos. EL antivirus hay veces que no puede llegar a todos los sitios en el momento adecuado. Un antivirus no es la panacea contra cualquier ataque o amenaza de Internet. Al igual que un cinturón de seguridad no nos va a evitar un

accidente, un antivirus no resultará eficaz si el usuario no toma una serie de medidas de precaución mínimas.

A la hora de conectarnos a Internet, recibir correos electrónicos o intercambiar archivos mediante el eMule, no debemos olvidar que la prudencia es nuestra mejor consejera. Si en carretera no circulamos a 180 marcha atrás lloviendo y sin luces… ¿por qué vamos a arriesgarnos a abrir todos los ficheros que nos manden, a entrar en todos los links que nos ofrezcan y a aceptar cualquier archivo descargado? Aunque tengamos el cinturón de seguridad del antivirus, el accidente puede ocurrir si no obramos con la prudencia adecuada.

De todos modos, no vayamos a caer en el pánico. Sí, Internet tiene muchos riesgos, pero afortunadamente podemos aprender cuáles son, podemos preguntar a expertos que nos van a aconsejar y podremos disfrutar de Internet sin problemas. ¿Saben dónde están esos expertos? Pregunte en el Cibercentro, están mucho más cerca de lo que pensaba.

***Fernando de la Cuadra***
***Director de Educación de Ontinet.com,***
***Distribuidor en exclusiva de los productos ESET***

*Es tan sencillo como acudir a* *http://www.eset.com/onlinescan*

# ¿QUIÉN ES EL RESPONSABLE DE MI SEGURIDAD?

***Por Carlos Puente***

Hoy en día parece evidente que la Seguridad Informática va cobrando más y más importancia en el trabajo diario de nuestras empresas y en nuestro tiempo de ocio en el hogar.

Y es que probablemente todos y todas hemos sufrido alguna vez algún ataque de un virus, nos han saltado extrañas ventanitas emergentes mientras navegamos, incluso hemos tenido que llevar nuestro ordenador al servicio técnico para formatearlo perdiendo aquellos documentos tan importantes y las fotos de nuestras últimas vacaciones…

Por eso, parece que ya nos hemos acostumbrado a tener un antivirus instalado en nuestros equipos, con lo que nos quedamos muy tranquilos al sentirnos protegidos y fuera de todo riesgo, con esto ya está, ¿no?


Pues resulta que como todo buen informático ya en varias ocasiones he escuchado frases como "*pero si yo no he hecho nada…*", "*yo sólo estaba navegando por Internet…*", "*me bajé unos archivos de la mula…*", "*si yo tenía instalado un buen antivirus…*" **¿Y AHORA QUÉ?** ahora no me arranca el ordenador, he perdido mis fotos, mis recuerdos, los valiosos documentos de trabajo, no puedo entrar en mi correo electrónico, mi jefe me ha visto en unas fotos que no debía, o es que ni siquiera me he dado cuenta, pero están usando mi equipo en una "red zombie" para lanzar ataques de "phising" y estafas en Internet, o hasta me han robado unos eurillos de mi cuenta.

Puede parecer alarmante, pero no se trata de eso, no debemos cogerle miedo a la tecnología, sino ser conscientes de los riesgos a los que nos enfrentamos cada vez que encendemos un ordenador, cuando navegamos por Internet, y por lo tanto podamos ser consecuentes con nuestros actos y responsables de proteger nuestros propios datos, nuestra identidad y privacidad.

Aunque no nos lo creamos es exactamente lo mismo que en montones de situaciones cotidianas en la "vida real" ¿acaso no vamos andando por la acera en vez de por el medio del asfalto?, ¿se nos ocurre llevar el bolso abierto por la calle, colgando despreocupadamente a nuestra espalda?, ¿dejamos nuestras llaves de casa o del coche puestas en la puerta?, ¿le dejamos la cartera, las tarjetas a un completo desconocido?, ¿dejamos entrar en casa a cualquiera, en cualquier momento?, ¿dejamos nuestros hijos e hijas al cuidado del primero que pasa?

Estoy seguro que si le damos nuestra tarjeta de crédito con su código pin a un desconocido que llama a la puerta de nuestra casa, simplemente por que dice venir de parte de nuestro banco, no vamos a poner una denuncia contra el banco porque ese "desconocido" nos haya vaciado la cuenta.

De la misma manera, si cogemos nuestras fotos privadas y las vamos poniendo por la calle a modo de carteles, o las dejamos en un banco del parque para que nuestras amigas y amigos puedan verlas… ¿nos sorprenderíamos de que las hubieran visto otras personas que no deberían?, ¿de que alguien nos las hubiera robado?, ¿de que las hubieran pintarrajeado o estropeado?

Ejemplos tan sencillos como éstos, en los que probablemente ninguno caeríamos en la "vida real", se producen de forma continua a través de la Red... pero… **¿QUÉ PODEMOS HACER?** En primer lugar:

***Ser igual de conscientes de los riesgos y peligros*** de las Tecnologías de la Información que de los que nos encontramos en nuestro día a día. Tus datos personales, de perfiles, correo electrónico, messenger, etc. te identifican para lo bueno y para lo malo, por lo que debes hacer un uso muy cuidadoso de ellos y no darlos indiscriminadamente.

***Asegura tu entorno informático***. ¿Te irías de viaje con un coche averiado, al que de vez en cuando se le bloquea la dirección o los frenos? Entonces, procura mantener limpio tu ordenador, con el sistema operativo y las aplicaciones actualizadas y configuradas correctamente.

***Piensa antes de actuar***. ¿Acaso firmarías un contrato de servicio de telefonía o de gas sin saber a qué te comprometes?, pues antes de instalarte un software, registrarte en un sitio web, o acceder a un nuevo servicio, hazte consciente de por qué te quieres registrar en él, para qué sirve, qué ventajas y posibilidades te aporta, qué datos personales necesitan, cómo los van a utilizar, qué riesgos puede implicar…

***Configura las opciones de seguridad y privacidad***. Está muy bien que tu coche lleve airbag de acompañante… pero ¿sirve de algo si lo tenemos desconectado? Todas las herramientas informáticas y servicios web como por ejemplo los correos electrónicos o las redes sociales (hotmail, gmail, facebook, myspace, hi5, tuenti, etc.) permiten configurar sus niveles de seguridad y privacidad, como por ejemplo a quién dejo ver mi información, qué información se va a mostrar de mí, etc.

***Infórmate y ponte al día en materia de seguridad informática***. La información es la mejor vacuna contra todo tipo de problemas. Si tienes dudas, consulta a un experto.

En resumen los ordenadores, los móviles, las PDAs, el correo electrónico, los clientes de mensajería instantánea, chats, blogs y redes sociales, entre otras, son poderosas herramientas a tu disposición, abriéndote un mundo de posibilidades, pero recuerda que eres tú quién debe saber utilizarlas y aprovecharlas adecuadamente, siempre siendo consciente de sus riesgos y consecuente con tus actos.

***Carlos Puente***
***Técnico de Fundación Dédalo***

**Nuestro más sincero agradecimiento a cuantos han hecho posible este BoleTIC, desde las personas, empresas y entidades que han participado, colaborado o patrocinado las actividades de la III Semana de Seguridad Informática, con una mención especial para los autores de los artículos recogidos en esta publicación.**

**Desde Fundación Dédalo queremos agradeceros a todos los Socios y Socias del Cibercentro de Tudela vuestra confianza y animaros a utilizar Internet y las Nuevas Tecnologías de forma segura.**
**Por ello os invitamos a visitar la Web:**
**http://seguridad.fundaciondedalo.org/**

**Para cualquier duda os podéis poner en contacto con nosotros en:**
**info@fundaciondedalo.org**
**www.fundaciondedalo.org**
**tlf.948.088.044**

Dèdalo
FUNDACIÓN

Colaboran: UNED TUDELA · INTECO Instituto Nacional de Tecnologías de la Comunicación · PantallasAmigas · CTIC · Informática 64 www.informatica64.com · AENOR · Día de Internet 17

Participan: Ontinet.com · eset · Diario de Noticias Eres lo que lees · EUROPA FM 99.1 · Plaza Nueva · Ribera navarra · Punto Radio 96.0 Fm Tudela · La Voz de la Ribera · Onda Cero 107.2 Ribera