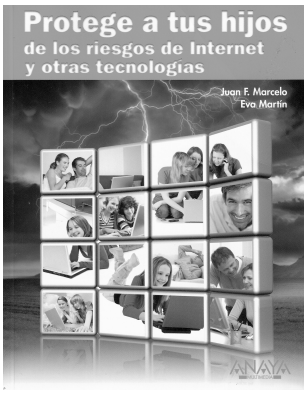
El lado oscuro de la Red

POR **GLORIA GÓMEZ-ESCALONILLA**



Protege a tus hijos de los riesgos de Internet y otras tecnologías
Juan F. Marcelo y Eva Martín
Madrid: Anaya Multimedia, 2010, 384 p.
ISBN: 978-84-415-2739-3

El tema principal del libro de Marcelo y Martín es el de los peligros que nos acechan cuando manejamos las tecnologías, especialmente Internet. Y es que conviene no olvidar que, al tiempo que la informática, la Red o los móviles ofrecen numerosas ventajas y comodidades, también pueden suponer serias amenazas o riesgos tanto para los propios equipos como para nuestro trabajo e incluso para nuestra propia integridad.

A pesar de destacar ese 'lado oscuro' de las nuevas tecnologías, el libro no se sitúa en el paradigma apocalíptico. Más al contrario. Porque si bien trata de todos esos riesgos, también ofrece la manera de evitarlos. Desde este punto de vista se puede decir que es un libro eminentemente práctico, casi rozando el 'manual' de seguridad.

Para aquellos que entendemos la informática en su uso más elemental, puede ser útil porque nos guía paso a paso con todas las indicaciones e instrucciones que tenemos que realizar para incrementar la seguridad de nuestros equipos. El problema es que la informática avanza tan deprisa que su utilidad tiene fecha de caducidad, y una fecha muy fugaz, porque es muy posible que cuando pongamos en práctica sus consejos y utilidades ya hayan surgido nuevas amenazas o nuevas versiones de las soluciones que aportan. No obstante, el libro sigue siendo útil para tener una noción de todo lo que nos acecha cada vez que encendemos el aparato,

porque en cada capítulo los autores nos detallan los peligros más habituales y los remedios para minimizarlos.

Actuación frente a los virus

La primera amenaza que tratan es la más común: los virus y otros códigos maliciosos que pueden hacernos mucho daño, y a todos nos puede llegar -o nos ha llegado ya- el virus fatal en el peor momento de trabajo y sin copia de seguridad. Frente a esta situación, que supone la peor de las pesadillas, los autores nos aconsejan realizar periódicamente *backup*, por si acaso los antivirus no son efectivos o nos llegan virus inmunes a nuestras protecciones. También nos piden extremar el chequeo por las puertas principales de entrada: correo, USB o intercambios P2P. Porque hay, como nos cuentan en este capítulo, numerosos virus, también gusanos, troyanos, ladillas, secuestradores, capturadores de teclado e incluso antivirus que camuflan virus.

Afortunadamente hay todo tipo de vacunas, antivirus, escáneres y cortafuegos que los autores nos aconsejan utilizar y nos indican cómo instalarlos e incrementar con ello la seguridad de nuestro equipo. De esta manera nos describen los antivirus más populares -como el Panda o el Norton- y otros más efectivos pero menos conocidos, como el Virus Total o el ClamWin; incluso opciones más económicas, pues también hay antivirus gratuitos y en línea que nos pueden servir. A esta batería de vacunas hay que añadir toda la gama de escáneres y cortafuegos, aunque si el usuario quiere un integrado puede hacer uso de las llamadas *suite* de seguridad, programas que cubren todas las necesidades de protección de los equipos. No hay excusa, pues, para estar expuesto a un problema de este tipo.

Ciberdelincuencia

Pero no solo existe este problema. Hay otras invasiones informáticas quizá menos peligrosas pero más insistentes y pesadas. Y entre estas invasiones están los *spam* y otros mensajes no deseados, como bulos u *hoax*, falsas as de virus, cibermendigos, troyanos, *spyware* o programas de vigilancia o *phising* bancario, mensajes todos ellos que nos llegan a pesar de los filtros de seguridad. Intrusos que nos llegan sin llamarlos, o sin querer llamarlos, porque a veces se nos cuelan por estar inscritos en determinadas listas de distribución, redes sociales, o simplemente por haber rellenado un cupón en la tienda de la esquina.

Decenas de correos diarios, miles si no tenemos filtros activados, que quieren vendernos algo, saber de nosotros, robar nuestro dinero o engañarnos para fines más perversos. En el mejor de los casos -y en la mayoría de ellos- solo nos molestan, pero puede ser peor. De hecho, el delito más frecuente en las redes no es la pornografía, aunque sea el más mediático, sino el *phising* bancario, el robo de dinero a través de correos falsos.

Efectivamente, las nuevas tecnologías representan nuevas maneras de robar y quizá una forma más directa de extorsionar, sobre todo por el acceso que tienen a nuestra intimidad y a nuestra vida privada; pero hay que tener claro a este respecto que las nuevas tecnologías no son malas en sí mismas. Como señala Joan Mayans, presidente del Observatorio para la Cibersociedad, «Internet no es ni más ni menos moral, peligroso, obsceno o divertido de lo que

somos sus usuarios» (*El País*, 2 de diciembre de 2010). Y es una reflexión que no queda clara en el texto que se presenta, pues este abunda en la facilidad de las tecnologías para la delincuencia, cuando los delincuentes son las personas que las utilizan.

Además, hay que tener en cuenta que esos delincuentes buscan gente incauta y vulnerable, y la mayoría de los usuarios de Internet, incluso los más pequeños, no lo son. En la mayoría de los casos sabemos qué hacer o no hacer ante ciertos requerimientos sospechosos. Cuenta el libro, y es cierto, que ha habido casos de *ciberbulling*, usurpación de identidades o acoso cibernético (aquí en España el del gaditano B.C.S., cuya amenaza de difundir imágenes de la adolescente que engañó provocó que aquella finalmente se suicidara); pero esos casos no dejan de ser meras anécdotas. Hay que repetir, frente a la visión que se propone desde el libro, que la mayoría de la gente utiliza la Red para comunicarse y relacionarse, no para delinquir.

No obstante, hay que extremar las as, sobre todo porque existe un riesgo mucho menos evidente pero mucho más extendido y quizá peligroso, que es el rastro que dejamos cuando navegamos, datos que dejamos de manera voluntaria y pistas que dejamos sin querer. Efectivamente, ahora están creciendo las as de las imágenes o datos que se cuelgan en las redes sociales y que pueden perjudicar en otros contextos, por ejemplo en el laboral. Y ello sin hablar de las *cookies*, esas piezas de texto que el navegador almacena sobre las preferencias del usuario en esa página web y que, aunque se pueden eliminar, la mayoría de los usuarios no lo hace y va dejando su historial para quien quiera mirar.

Así pues, quien quiera espiarnos nos puede espiar, y los autores del libro señalan que «hay un espionaje masivo, que no solo se lleva a cabo con el conocimiento de los gobiernos sino con su complicidad» (p. 219). Podemos pensar que a nadie le interesa nuestra vida, pero no es del todo verdad. Los autores afirman, de hecho, que «los servicios gratuitos de correo, de relaciones, de búsqueda de trabajo o de redes sociales son en realidad grandes reservas de datos que posteriormente sirven para elaborar perfiles publicitarios» (p. 17). Hay que protegerse, pues, y defender el derecho a la intimidad frente a las intrusiones, pero también frente al gran escaparate que supone la Red.

El control de los padres

Por eso resulta interesante este texto, porque nos percatamos de nuestra vulnerabilidad en el nuevo escenario digital. En realidad, cuando uno lee este libro se da cuenta de la suerte que ha tenido porque no le haya pasado nada grave, aunque si se aplica el sentido común y se activan los controles mínimos de seguridad el riesgo se minimiza bastante. Incluso entre los más pequeños.

El libro detalla en un capítulo las protecciones que podemos activar para proteger a nuestros hijos, desde la más básica de establecer claves de usuario hasta el sistema de ‘control parental’, que permite bloquear el acceso a los juegos, programas o sitios web no aptos para menores, limitan el tiempo que les permite conectarse o proporcionan informes del historial de navegación. Realmente este programa parece un ‘*supernanny*‘ digital que nos ayudará a educar a nuestros pequeños; aunque también podemos contratar un sistema de filtrado a las operadoras de red para que bloqueen las páginas con ciertas palabras no apropiadas para los

menores: pornografía, violencia, sectas, drogas…

Pero lo más importante es tener en cuenta que esas herramientas no sirven si el menor las desactiva o las puentea, cosa que puede pasar cuando la Red seduce a nuestros adolescentes. Realmente, esa es la etapa más vulnerable -como en la vida real-, sobre todo ahora que han trasladado sus relaciones al ámbito virtual y ya no es el parque el escenario principal de su socialización, sino el Tuenti o Facebook, con miles de amigos, con miles de datos expuestos a todo el mundo, con códigos que solo entienden ellos mismos.

No se pueden poner puertas al campo y por mucho control parental que exista, lo normal es que en las nuevas tecnologías domine el adolescente. Le ayuda el carácter anárquico de la Red y su inmersión. Son nativos digitales. Y un ejemplo paradigmático, que el libro también menciona, son las páginas de ‘ana y mía’, páginas que incentivan la anorexia y la bulimia y que, a pesar de las presiones de las asociaciones para eliminarlas y de los controles de los padres y madres para filtrarlas, las adolescentes de todo el mundo siguen navegando por ellas, y muchas a la deriva.

Lo que hay que hacer, como concluyen los autores, es educar, formar y enseñar en el uso responsable de las nuevas tecnologías, aunque no haya herramientas informáticas que nos ayuden a ello.

En definitiva, el libro de Marcelo y Martín ofrece una excusa perfecta para reflexionar sobre lo que nos puede pasar -a nosotros y a los nuestros- cuando utilizamos las nuevas tecnologías, porque a pesar de que el uso normal y común favorece su faceta más lúdica, su facilidad para descubrir nuevos mundos y nuevas relaciones, facilitarnos el trabajo y buscar información, también podemos tener experiencias negativas que podemos evitar extremando precauciones e incrementando la seguridad. Este libro advierte, pues, para no tener que lamentar.