En definitiva, los autores realizan una reflexión sobre el papel de la información y los medios de comunicación online en las bibliotecas, una tarea que ha evolucionado desde las antiguas carpetas de ejemplares de periódicos a las pantallas y las redes sociales.

Itxaso Fernández Astobiza

Cómo protegernos de los peligros de Internet

Gonzalo Álvarez Marañón, (2009)

Madrid: CSIC

Internet ha supuesto la transformación radical de los ritmos vitales de una parte de la ciudadanía. Junto a la mejora en tareas antaño laboriosas (como la comunicación entre personas, o con la Administración) han surgido también dificultades que obstaculizan la percepción 'bondadosa' de la nueva herramienta: fraudes en las transacciones comerciales, invasión de la intimidad, difusión e intercambio de contenidos de abusos con menores... El autor, Gonzalo Álvarez Marañón, investigador del Centro Superior de Investigaciones Científicas (CSIC), presenta en esta obra las vías a través de las que se 'cuelan' en los equipos informáticos los peligros más extendidos y ofrece, al mismo tiempo, una amplia gama de mecanismos de protección para hacerlos frente.

Explica que, a estas alturas de su evolución, el riesgo en indisociable de la propia red, por lo que hay que aprender a convivir con él, sabiendo cómo gestionarlo. Para ello hay que considerar el entorno doméstico de cada cual: presencia o no de menores o jóvenes, nivel de conocimiento como usuario, calidad de la conexión, tipo de uso de la red...

Como gran parte de la vida y actividad de mucha gente gira en torno a una CPU, se recomienda no escatimar en medidas de seguridad, tanto cara al exterior como ante las disfunciones de los equipos propios. La seguridad deberá ser tanto más protectora cuanto más valioso sea el bien (o archivos) a preservar.

Cualquier usuario de la red puede ser víctima de alguna de las amenazas que pululan en ella: desde la acción de un *hacker* que pretende husmear en el disco duro, o la instalación de alguna aplicación invisible de software malicioso (*malware*), hasta los fraudes comerciales, etc. En el libro se indica cuáles suelen ser los principales objetivos de los *ciberatacantes*, qué caminos utilizan (*phishing, spam*...) y mediante qué procedimientos localizan a sus víctimas.

Así, respecto al *malware* (virus, gusanos y troyanos), se exponen las medidas básicas de seguridad —aquellas "que no pueden faltar en ningún hogar"—, que se basan en el uso de cortafuegos, de antivirus y en una actualización sistemática de ambos, factor éste sumamente importante y que habitualmente suele descuidarse.

Otras sofisticadas amenazas que también deben evitarse son el 'correo basura' o *spam*, el *adware* o publicidad agresiva a través de ventanas emergentes (*popups*) o fijas (*banners*), el *spyware* o aplicaciones 'espías' que se instalan en nuestros equipos sin permiso ni aviso previo o, también, la accesibilidad indiscriminada a contenidos pornográficos o violentos por parte de los menores; para evitarlas existe una gama de productos denominados de 'control parental', que filtran muchos de ellos e impiden su accesibilidad.

Casi siempre el objetivo último es mantener bajo control el contenido de los dispositivos de almacenamiento, comenzando por el del disco duro interno del ordenador, hasta el de los *pendrives* u otros discos externos. El autor advierte de que, hoy por hoy, no existe procedimiento alguno que proteja al cien por ciento, ya sea porque los sitios web amenazantes cambian constantemente, porque la configuración de los productos de protección es demasiado compleja, o porque junto a la desactivación de los contenidos 'maliciosos' se bloquean también otros inocuos.

Además de estas medidas básicas de protección, se recomienda mantener los contenidos de los equipos siempre a salvo mediante las copias de seguridad (*backup*), tanto los datos asociados a las

aplicaciones (favoritos, preferencias, contactos...), como los archivos personales (textos, vídeos, música...). Se precisará para ello de soportes de almacenamiento adecuados, desde el básico DVD regrabable, hasta los discos externos de 500 GB, 1.000 GB, o de mayor capacidad.

Una de las secciones más interesante del libro es la referida a la protección de la privacidad y del anonimato de los internautas. Aunque de partida se advierte de que "la intimidad en Internet no existe", se proponen varias herramientas para tratar de mitigar la indefensión: la criptografía o cifrado de los datos, el borrado 'definitivo' de los archivos eliminados —y no sólo de su rastro—, la navegación (cuasi)anónima a través de direcciones URL intermediarias, la supresión de las huellas de navegación en el propio equipo... En este sentido, se avisa también de las precauciones a tener en cuenta al acceder a Internet a través de una red Wi-Fi: si no se protegen mediante contraseñas las redes domésticas, se corre el riesgo de que cualquiera que se encuentre dentro de su cobertura pueda espiar todo el tráfico de datos; en sentido inverso, si se accede como "gorrón" a una red Wi-Fi abierta ajena, deberá cuidarse también la información transmitida, ya que ésta puede ser espiada por el administrador propietario del sistema.

Respecto a las conocidas y populares redes sociales, como Facebook o Tuenti, Álvarez Marañón advierte de que, junto a las innegables ventajas, platean también innumerables interrogantes sobre su seguridad, por lo que suponen de amenaza para la intimidad y privacidad de las personas. De una parte, aquellos contenidos (fotos, vídeos...) de tipo personal que inconscientemente se 'suben' abiertos a todo el mundo; de otra, la posibilidad de convertirse en el medio para el *ciberbullying*, o acoso entre iguales. Ante estos peligros, el autor nos presenta hasta una decena de prácticas recomendaciones.

Un aspecto que quizás pudiera haber sido mejorado es el relativo a las especificidades de los diferentes sistemas operativos; aunque la eventualidad de los peligros de Internet no representa lo mismo en cada uno de ellos (Windows, Linux, Mac OS...), los remedios se han presentado de manera uniforme, entreviéndose el protagonismo de las soluciones para el entorno Windows sobre las demás.

En definitiva, a lo largo de seis capítulos y lejos de pretensiones de divulgación científica o académica, la obra se presenta, tal como el propio autor apunta, como "un libro para el usuario doméstico", en el que impera la claridad y la sencillez en la exposición de los argumentos. Difícilmente podrán encontrarse más consejos para la seguridad de los navegantes en las poco más de cien páginas con las que cuenta.

Juan Carlos Pérez Fuentes

Redacción informativa en prensa

José Ignacio Armentia Vizuete y José María Caminos Marcet (2009)

Barcelona: Ariel

¿De qué depende que un periodista elija o no un acontecimiento? ¿Es infinita la libertad de información? ¿Qué factores influyen a la hora de optar por un titular informativo determinado?¿Cómo surge la figura del Defensor del Lector y cuál es su labor en los periódicos actuales? ¿De qué manera ha contribuido el periodismo digital al nacimiento de nuevos géneros periodísticos inexistentes en la prensa escrita tradicional?

A estas y más preguntas responden José Ignacio Armentia y José María Caminos en su libro Redacción Informativa en Prensa. En esta obra los autores hacen un examen del mundo de la prensa, la redacción periodística, sus normas y tendencias, que resulta de gran utilidad para los estudiantes de Ciencias de la Información y los profesionales del mundo del periodismo.

El libro está compuesto de once capítulos. Cada uno de los diez primeros aborda un tema específico relacionado con la profesión. Los capítulos se inician con una reseña de las competencias a adquirir con su lectura, y al final de ellos se proponen unos ejercicios prácticos sobre el tema en