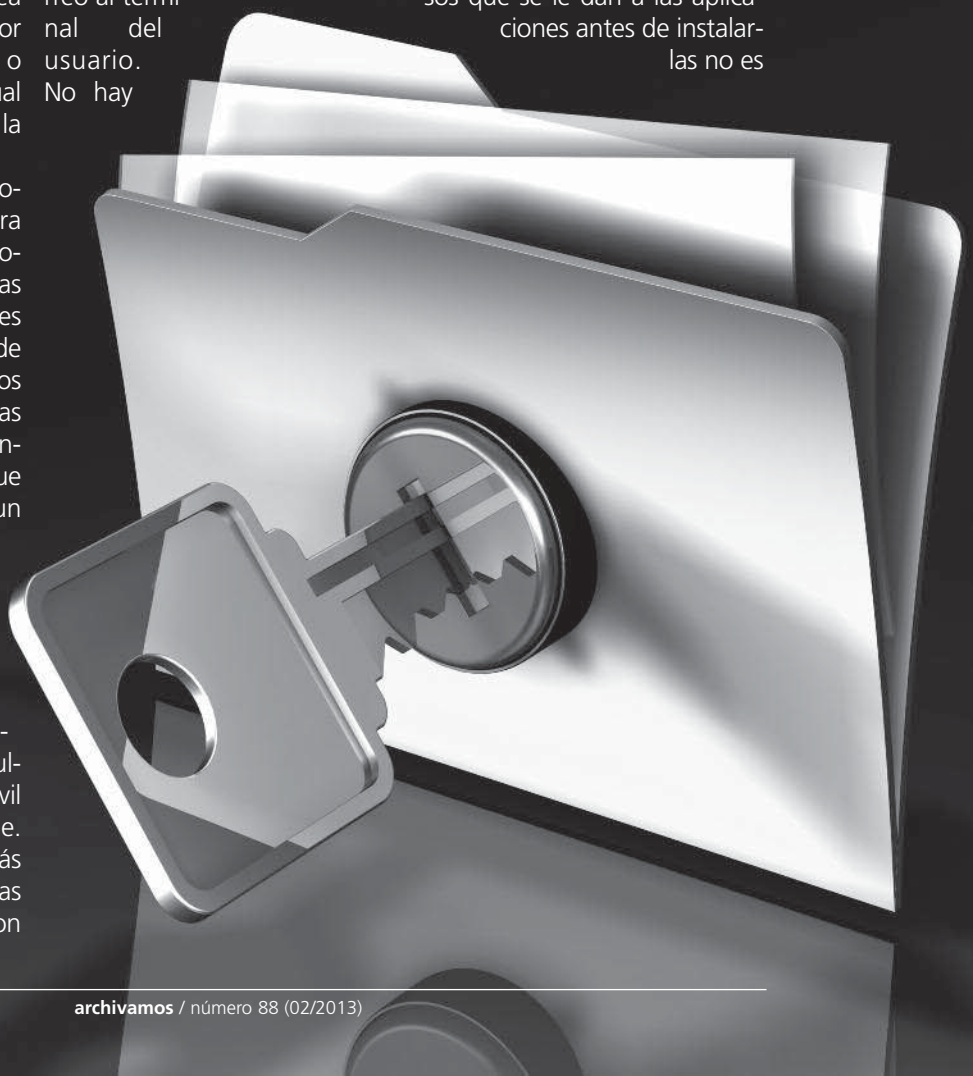
Privacidad virtual, ¿bajamos la guardia?

David Herreros Díez

Es un consejo recurrente recomendar siempre leer la letra pequeña de los contratos para evitar posteriores sorpresas desagradables. Este consejo cobra una especial relevancia si se traslada a leer los términos y condiciones de los programas o aplicaciones que instalamos en nuestros sistemas informáticos o dispositivos móviles

Cuántas veces nos ocurre a lo largo de nuestra vida que no leemos la letra pequeña de los contratos que firmamos, bien sea para abrir una cuenta corriente o decidir hipotecarse durante 30 años. ¿Leemos las cláusulas cuando nos hacemos socios de un gimnasio? ¿Revisamos a fondo las condiciones de un contrato? En más ocasiones de las deseables la respuesta suele ser no. ¿Qué ocurre actualmente en un mundo donde ya gran parte de los trámites los realizamos a través de Internet? ¿Obramos dándole locamente a aceptar sin leer lo que realmente estamos aceptando? Es habitual que la respuesta sea que por descuido, prisas, por no entender lo que leemos o por desidia, funcionemos igual en el mundo físico que en la gran aldea global de Internet.

Con la proliferación exponencial de las aplicaciones para móviles son muchas las personas que se lanzan a instalarlas sin pararse a revisar a qué les están dando permiso. Varias de estas opciones en los permisos son potencialmente peligrosas como la de permitir enviar mensajes, ya que no olvidemos que esta acción suele conllevar un coste económico y más si se trata de SMS Premium, solicitar permiso para llamar directamente a otros usuarios, tener acceso al historial de páginas que visitamos, con lo que nuestra privacidad respecto a qué consultamos en la Web desde el móvil se convierte en algo vulnerable. Quizás las dos opciones más habituales requeridas por las aplicaciones para móviles son solicitar el acceso total a Internet y administrar las cuentas del usuario. En el primer caso se le daría permiso a una app maliciosa instalada por desconocimiento de sus intenciones reales a tomar el control de nuestro terminal y en el segundo caso podría conllevar la posibilidad de que una aplicación elimine o añada cuentas de correo al terminal del usuario. No hay que olvidar la opción que permite a la aplicación tomar fotos o videos con la cámara del teléfono sin el conocimiento del usuario ya que al instalarla le hemos dado permiso para ello. Si bien es cierto que generalmente las compañías que se hallan detrás no harán un uso ilegitimo o fraudulento con esas apps, sin duda leerse los permisos que se le dan a las aplicaciones antes de instalarlas no es



un asunto baladí y conviene fijarse bien antes de aceptar. Comienzan a conocerse casos como el de la aplicación gratuita del juego del Monopoly distribuido a través de un famoso canal de descarga de apps que tras su instalación enviaba desde el terminal de los usuarios SMS Premium con un coste considerable para ellos. Durante los últimos meses se ha ido dando un aumento exponencial de delitos relacionados con la intimidad de las personas en la Red, habiendo solo durante el 2012 un total de 750 personas detenidas por delitos tecnológicos.

Alessandro Acquisti, economista del comportamiento en la Universidad Carnegie Mellon en Pittsburgh, estudia el comportamiento de las personas ante la defensa de su propia privacidad en la Red. En una serie de experimentos sociológicos, ha demostrado que a pesar de lo mucho que los usuarios aseguramos valorar nuestra privacidad, tendemos a ignorar las precauciones lógicas que habría que tomar para protegerla de una manera incomprensible. Algunas de sus últimas investigaciones muestran cómo a los usuarios de Facebook les ha llevado 7 años lograr que el gigante informático endurezca sus ajustes de privacidad o que en la actualidad muchas empresas utilicen cada vez con mayor intensidad las redes sociales para discriminar candidatos a puestos de trabajo que ofertan.

Durante otra investigación en 2011, tomó fotografías con una cámara a cerca de 100 estudiantes en el campus donde trabaja. En cuestión de minutos, había identificado alrededor de un tercio de ellos gracias al uso de software de reconocimiento facial de una conocida red social. Además, alrededor de una cuarta parte de los sujetos a los que se pudo identificar, mostraban en el perfil de esa red social suficiente información como para adivinar al menos una parte de su número de la Seguridad Social. El objetivo del experimento era demostrar lo fácil que es identificar a las personas gracias a la gran cantidad de datos personales que distraídamente dispersamos en la Web, como por ejemplo la fecha de nacimiento. Nuestros hábitos de navegación, términos de búsqueda, la comunicación por correo electrónico o los permisos que damos a las apps revelan bits de información que pueden ser usados con diferentes fines en función de en qué manos caigan.

La privacidad es un bien cada vez más escaso en el mundo digital. La incorporación a Internet de diferentes tipos de dispositivos móviles está derivando en la "era de sensores", según el ex consejero delegado de Apple, John Sculley, dispositivos que suman nuevas fuentes de información a quien se dedica a recopilarla para darle luego fines comerciales o de otro tipo. Según el mayor fabricante de dispositivos de conectividad, Cisco, al comienzo de la próxima década habrá 20.000 millones de dispositivos inalámbricos conectados –tabletas, smartphones además de cámaras y micrófonos– que estarán recopilando y generando datos sin parar. Desde el proyecto iWatch en el que podría estar trabajando Apple con sensores biométricos o las polémicas gafas de Google que podrían registrar todo lo que vea quien las lleve. Un registro íntimo de nuestra vida cotidiana cada vez mayor que está a la vuelta de la esquina y que sin duda desborda a los Gobiernos y organismos públicos a la hora de legislar su control.■