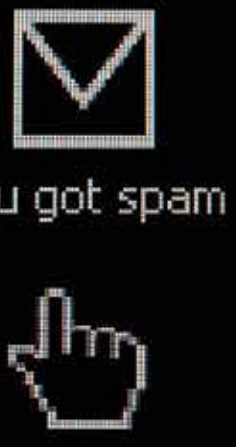
EL DOBLE FILO DE LA PRIVACIDAD EN INTERNET



LA TERCERA VEZ QUE MIRAS UNA HABITACIÓN DE HOTEL, ESTA HA SUBIDO DE PRECIO. SI HABLAS CON TU MADRE DE UN PRODUCTO POR WHATSAPP, RECIBES ANUNCIOS RELACIONADOS EN GOOGLE. ¿ESTÁN LOS MENSAJES REALMENTE ENCRIPTADOS? LO QUE DECIMOS, CON QUIÉN LO HABLAMOS Y CÓMO LO HABLAMOS CONSTRUYE UN PERFIL PERSONAL QUE CIRCULA VELOZ POR LAS MANOS ANÓNIMAS DEL MUNDO DIGITAL. Y CASI SIEMPRE CON LA INTENCIÓN DE HACER NEGOCIO.

Dónde estas, qué música escuchas, los archivos que descargas o qué dicen los mensajes que intercambias –y con quién–. Muchos internautas descartarían de plano otorgar permisos para que alguien tenga acceso a esta información personal, pero en realidad es muy probable que ya lo estén haciendo. Así lo afirma un reciente estudio coordinado por dos académicos españoles, Juan Tapiador, de la Universidad Carlos III, y Narseo Vallina-Rodríguez, de ICSI (Universidad de Berkeley, Estados Unidos), que analiza las aplicaciones preinstaladas en más de 1.700 teléfonos Android de todo el mundo (más del 80% del mercado).

Sucede continuamente. El *retargeting* (dirigirse a usuarios que antes han interactuado con una determinada marca) y las técnicas de venta por Internet son cada vez más sofisticadas, invasivas y opacas. Recaban datos de nuestras navegaciones y hasta del contenido de mensajes y correos electrónicos. ¿Dónde está el límite ético y legal? Fabricantes, operadoras, programadores y grandes comercios, entre otros, tienen acceso a los datos de los internautas y resulta casi imposible discriminar cuánto compartimos al navegar. Puede que las aplicaciones de Google Play nos pidan permisos de acceso, pero no es el caso de las que vienen ya instaladas junto al sistema operativo. Y el entramado de permisos va complicándose al actualizarse las *apps* e interactuar entre ellas. Programas espía, píxeles de control (imágenes que sirven para monitorizar la actividad en Internet), *cookies*...

"TODOS TENEMOS UN VALOR".

Sin duda alguna, lo más valioso del mundo digital es el dato de los clientes. Las empresas digitales se valoran por el dato, y la lucha por él es encarnizada. La información extraída de nuestras navegaciones, las descargas, las valoraciones que dejamos y, por supuesto, nuestros comentarios en las redes sociales. "Todo lo que aportemos de nuestra vida digital (y no digital, pues la real es ya casi una extensión de la primera) es valioso para el sistema, hasta el punto de otorgarnos una puntuación como usuarios *(scoring)*. Todos tenemos un valor económico y, dependiendo de él, podremos disfrutar en el futuro de unos u otros servicios. Todo ya no es para todos", sostiene Jesús Hernández, experto en marketing digital.

Imagina que vas a solicitar un préstamo para un coche. En la actualidad, la entidad financiera vigila unos indicadores que tienen que ver con nuestra nómina, el historial crediticio, el aval que podamos aportar o nuestro saldo medio: todo un perfil que ayuda a reducir riesgos, pero que no garantiza la devolución del dinero prestado. Por ello, ya existen sistemas que ayudan a las entidades a saber más de los clientes. Nuestras navegaciones le dicen al sistema en dónde estamos, las fotos que subimos a las redes informan de nues-

tro estilo de vida y los comentarios hacen lo propio con nuestras conductas e intenciones. "Si al acceder a una red social los amigos con los que conversamos no son los más recomendables (desde un punto de vista financiero), si las fotos que mostramos no se han tomado en los mejores momentos y la conducta que reflejamos no es la más acertada, no será de extrañar que no nos den un préstamo o que no podamos acceder a ciertos servicios", argumenta Hernández, también doctor en Economía de la Empresa por la Universidad Rey Juan Carlos de Madrid. Los algoritmos de inteligencia artificial ya indican los tipos de palabras que introducimos en los textos, en los audios o en cualquier tipo de comunicación que hagamos. Y lo hacemos todos los días, continuamente, en redes sociales, WhatsApp, comentarios a noticias...

Frente a este ingente tráfico de datos, el usuario permanece en gran medida ignorante, "a menos que sea un experto y sepa cómo intercambian información los sitios web, qué es una *cookie*, el funcionamiento de la publicidad *online*... Hay un sistema complejo de intermediarios que incluyen pujas en tiempo real para que un determinado *banner* acabe en tu navegador, según los intereses del usuario", afirma Ángel Cuevas, investigador del departamento de Ingeniería Telemática de la Universidad Carlos III en Madrid.

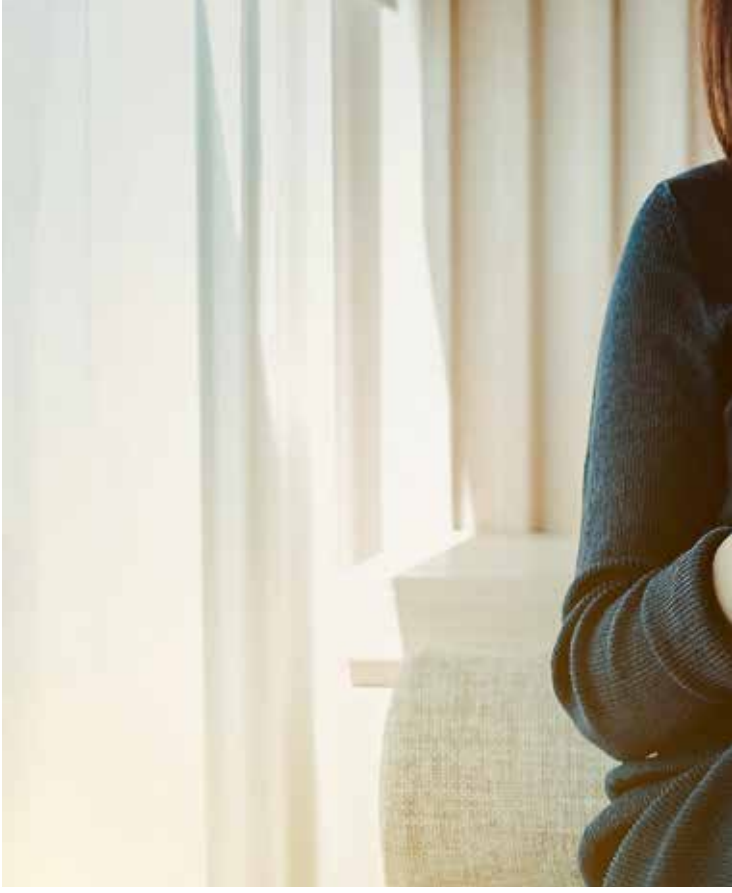
HAY QUE LEER ANTES DE ACEPTAR.

Internet no existiría sin la información que, consciente o inconscientemente, damos al sistema para que funcione correctamente, pero "también es cierto que nunca fue concebido comercialmente, ni para que fuera seguro ni privado", añade Hernández. De hecho, si lo fuera, nunca podríamos beneficiarnos de las ventajas que nos brinda y que en la mayoría de las ocasiones exigimos cuando nos conectamos a Internet. "En 30 minutos de navegación entregamos nuestros datos a más de 100 empresas de todo tipo", puntualiza.

Al unirnos a las redes sociales, hemos aceptado unos términos y condiciones en los que se especifica que todos los textos son analizados a través de herramientas de *machine learning* (inteligencia artificial). Muchas aplicaciones para móviles actúan de la misma manera para acceder a un determinado servicio, y el Reglamento General de Protección de Datos de la Unión Europea obliga a que se informe al usuario de todas las terceras partes que están en una web y qué tipo de información se comparte con ellas. "Otra cosa es que luego el usuario acepte los términos de uso sin leerlos. Al final, casi nadie lo hace por una cuestión de tiempo y de simplicidad", explica Cuevas.

'RETARGETING' O PRESENCIA RECURRENTE.

A estas alturas, ya no sorprende ver cómo nos suben el precio de un servicio o de un billete de avión cuando rea-



¿CÓMO RASTREAN NUESTROS DATOS?

Los primeros datos que se capturan son los denominados activos, aquellos que los usuarios damos voluntaria y conscientemente. El dato pasivo, por otra parte, se recopila sin que el cliente sepa qué información se está captando o con qué fin.

Las páginas web deben informar sobre las *cookies* que se insertan en sus navegadores, pero pocas personas se toman el tiempo necesario para entender su funcionamiento; conviene no aceptar ciegamente.

Pero ¿qué son esas *cookies?* **Se trata de pequeños archivos de identificación personal** que crea la página en la que nos encontramos y que son enviados y compartidos por una red de intervinientes repartidos por todo el mundo. Si visitamos la web de un producto y seguidamente navegamos a nuestro periódico favorito, recibiremos anuncios de productos relacionados.

Pero no acaba ahí: se hace además un monitoreo de toda nuestra actividad digital y se comprueba todo lo que pueda ser de interés. Como, por ejemplo, el tipo de dispositivo, la localización, las veces que entramos en una página, la frecuencia con que buscamos un producto e incluso las veces que mencionamos cierta palabra clave en nuestros correos o sistemas de mensajería.

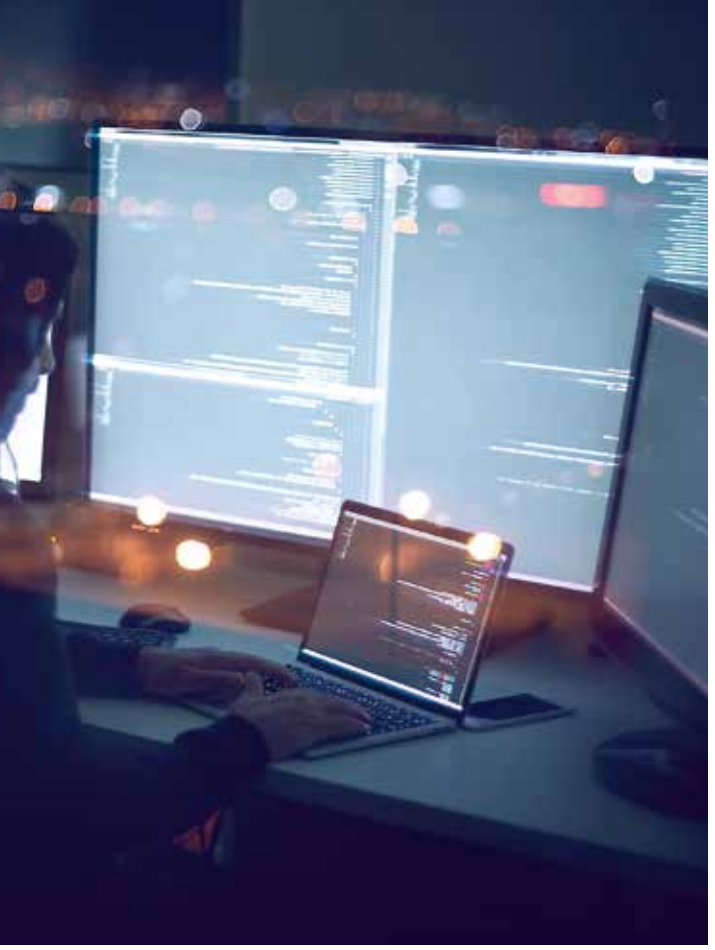
Internet no fue concebido para que fuera seguro ni privado. En 30 minutos de navegación entregamos información personal a más de 100 empresas.

lizamos la búsqueda en repetidas ocasiones. O que nos oferten un determinado producto que misteriosamente deseábamos y del que solo sabía alguien a través un simple mensaje de WhatsApp o un correo electrónico compartido. Y los mensajes publicitarios aparecen, muy convenientemente, también en webs que nada tienen que ver, aunque redes sociales como Facebook o Instagram ofrecen la posibilidad de notificar un anuncio demasiado recurrente. Este no desaparecerá, pero lo cambiarán por otro. En teoría, todo está encriptado para que nadie invada nuestra privacidad, "pero lo que no se garantiza es que esas *apps* no entreguen información acerca de nuestro comportamiento de consumo de forma anonimizada. Lo importante no es cómo te llamas o en dónde vives, sino cómo te comportas, qué dices, qué quieres, con quién te relacionas y por dónde navegas", comenta Hernández.

Nueve consejos para protegerte de los fraudes en Internet

(del Centro Europeo del Consumidor en España)

1. **Si parece demasiado bueno** para ser verdad, probablemente no lo sea.
2. **Si no has participado en un sorteo,** nunca podrás ganar un premio. Y si te piden dinero por adelantado para cobrarlo, sospecha de fraude.
3. **Desconfía si te piden tu cuenta bancaria,** tarjeta de crédito u otra información confidencial. Recuerda que los bancos nunca solicitan datos financieros por teléfono o correo electrónico.
4. **Si la persona que te ha contactado** parece más emocionada de lo que puedas estar tú mismo o actúa como si fuera una amiga íntima, hay gato encerrado.
5. **Cuando un determinado producto se oferta** a un precio muy por debajo del mercado, cuidado. Puede ser una estafa.
6. **Si te dicen** que debes responder de inmediato o el dinero será entregado a otra persona, recela.
7. **En el caso de que hayas abonado dinero,** no envíes más, notifícaselo a la policía y acude al banco; si usaste una tarjeta bancaria pueden ayudarte a reclamar.
8. **Si albergas dudas acerca de la legitimidad** de una empresa, búscala en Google junto a términos como "opiniones", "comentarios" o "estafa".
9. **Antes de comprar un producto,** visita la web de la empresa, verifica el teléfono de contacto y comprueba que no contiene errores lingüísticos; suelen ser señal de actividades fraudulentas.



EL PELIGRO DE LAS ESTAFAS 'ONLINE'.

Según el Ministerio del Interior, en 2017 se cometieron 81.307 ciberdelitos en España. De ellos, 60.511 (el 74,4%) están relacionados con diferentes tipos de fraude informático (estafas bancarias, de tarjetas de débito o crédito...). *Phishing*, cartas nigerianas, depósitos de garantía, falsas loterías... La lista es extensa, por lo que conviene saber cómo actuar si somos víctimas de alguno.

El 'phishing'. España fue el tercer país del mundo que más ataques de esta estafa recibió en el último trimestre de 2018 (17,5% de los internautas), solo por detrás de Guatemala (19%) y Brasil (18,6%), según la empresa de ciberseguridad Kaspersky Lab. Los delincuentes se hacen pasar por entidades financieras que necesitan verificar los datos del usuario, para lo cual le piden que confirme o actualice información personal sensible como números de tarjetas, nombres de usuario o contraseñas de acceso. Usan, para ello, páginas web de apariencia similar a la de su banco real, con el objetivo de engañar al usuario y acceder a su cuenta bancaria. Si se recibe un correo de estas características, es fundamental no responder ni pinchar en el enlace, ya que no es legítimo: los bancos nunca solicitan este tipo de datos. Para protegerse, conviene usar un *firewall* y antivirus, y mantenerlo siempre actualizado.

En 2017 se cometieron 81.307 ciberdelitos en España. El 74,4% están relacionados con diferentes tipos de fraude.

Cuidado con las cartas nigerianas. ¿Qué harías si recibes un correo ofreciéndote un negocio extremadamente lucrativo? En este tipo de fraude, llamado así porque originalmente los estafadores decían provenir de Nigeria o de otros países africanos, una persona desconocida que asegura ser familiar o representante de alguien recientemente fallecido busca ayuda para transferir al extranjero una considerable cantidad de dinero que dejó esta persona, ofreciendo a cambio una buena comisión; solicita discreción y le pide que abra una cuenta bancaria para remitirle el dinero.

Para convencer a la víctima, le manda documentos en apariencia auténticos y, cuando ya cuentan con su confianza, le comunican que han surgido unos problemas para cuya solución es necesario el pago de unos impuestos o tasas especiales. Es el comienzo de una sangría económica que alcanza cantidades millonarias: el año pasado, la Policía Nacional desarticuló una banda criminal que llevaba a cabo esta estafa en 17 países y que llegó a defraudar más de seis millones de euros.

Si recibes una comunicación de este tipo, no contestes ni envíes datos bancarios ni personales. Si has llegado a enviar algún dinero, guarda toda la documentación y contacta con la policía.

Las falsas loterías. La página oficial de Loterías y Apuestas avisó sobre las diferentes formas de este timo. La víctima potencial recibe un correo en el que se le comunica que ha ganado la lotería, a pesar de no haber participado en sorteo alguno. Para recibir el premio, ha de confirmar su identidad rellenando un formulario y adjuntando copias del pasaporte o DNI, y luego elegir entre una transferencia bancaria, abrir una cuenta en una entidad determinada o recogerlo en persona (en un país muy alejado). La mayoría de las víctimas escogen la primera opción, para lo cual será entonces necesario el pago por adelantado de tasas, honorarios legales... Como en otras estafas, es vital no responder a estas comunicaciones, no enviar dinero ni adjuntar copias de documentos de identidad, guardar toda la documentación relevante y, por supuesto, contactar inmediatamente con las autoridades.