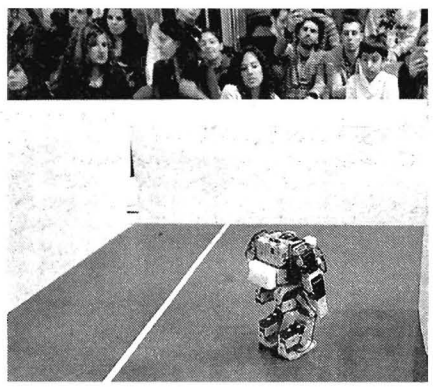
G/U/CAMPUS

23 / NOVIEMBRE / 2011 / Nº 37

EMPLEO VERDE
Dos leoneses convierten los residuos lácticos en abonos

HOMECINEMAD
El cine más alternativo se proyecta en los mejores salones

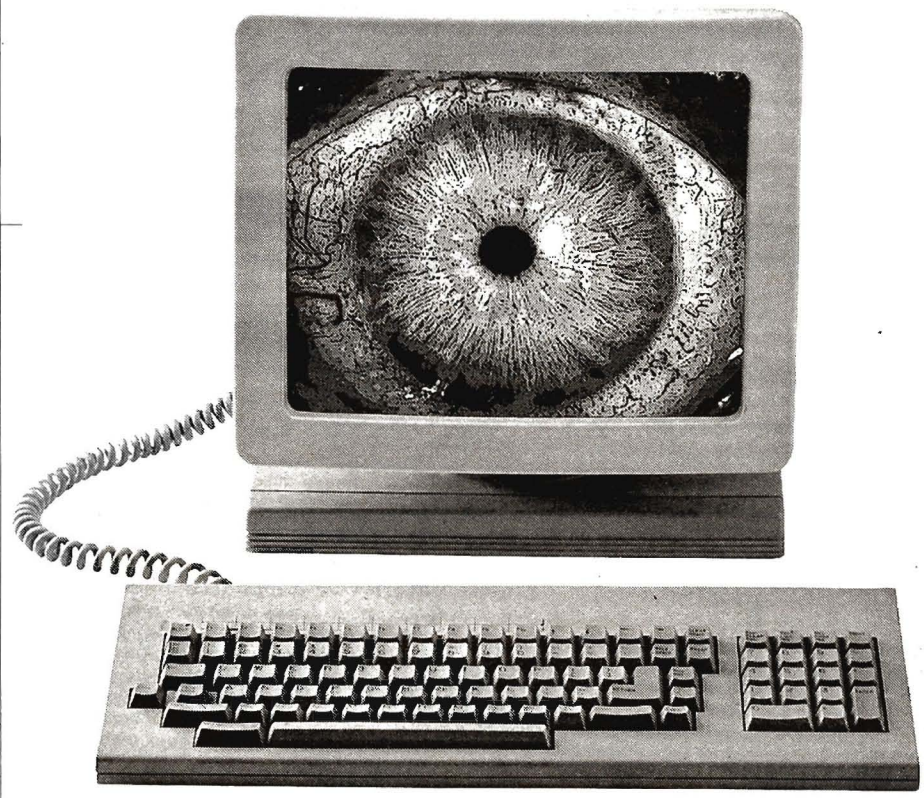
LOS ROBOTS SALTAN AL RUEDO EMPRESARIAL



Mientras Madrid acoge la Semana Europea de la Robótica, un concurso en Barcelona ha permitido a los apasionados de estos 'humanoides' mostrar sus últimas creaciones en un campo con gran proyección que aúna la electrónica, la informática, la ingeniería, los materiales y las baterías.

6

ESPIONAJE VIRTUAL. Fotos, información bancaria... Así son las 'bases de datos' más íntimas de la red

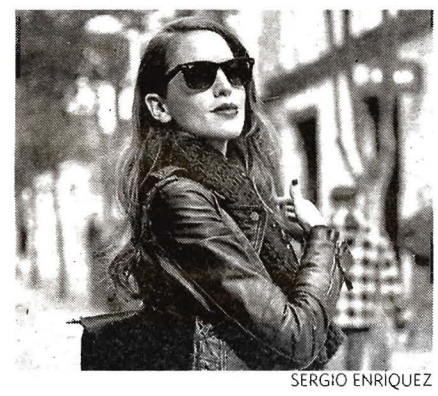


LUIS PAREJO

La reserva de entradas para un concierto, las fotos de un viaje o la solicitud de trabajo. Todo se lleva a cabo ya por internet. Entre el mito de la inseguridad de pagar online con tarjeta de crédito y la realidad de que nuestras cuentas y datos personales puedan ser *hackeados*, se encuentran numerosas acciones cotidianas que pueden poner en peligro nuestra privacidad.

Mientras que cierta información personal es compartida de manera controlada y libre, especialmente en las redes sociales, algunas empresas asociadas al marketing y la pubilcidad atraen a los usuarios con juegos, tests y servicios para acceder a sus datos y elaborar valiosas bases de datos y perfiles. La máxima expresión del uso fraudulento de la información personal en la red es el *ciberacoso*. Elena, de 20 años, vio cómo alguien robó sus claves y su perfil de facebook para compartir archivos personales comprometedores a todos sus contactos. Amenazada, se pregunta cómo afectará a su futuro. / PÁGINAS 2 Y 3

LA ÚLTIMA MODA ES VERLO TODO MUY NEGRO

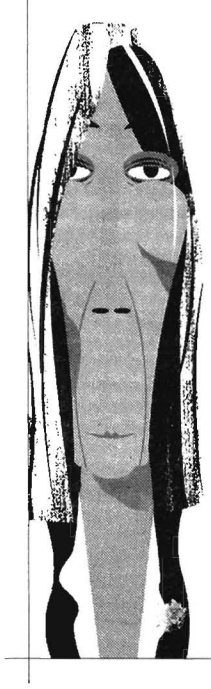


SERGIO ENRIQUEZ

No, el pesimismo no es lo más 'trendy', sino que el negro viene pegando fuerte esta temporada. Es un tono camaleónico que puede servir para una cena de gala como para una 'quedada' entre amigos. De la elegancia a lo más 'casual', pero siempre con un toque 'sexy' que no pasa de moda, el negro es el color.

8

M. KODAMA: «Creo que Borges nunca descansará en Argentina»



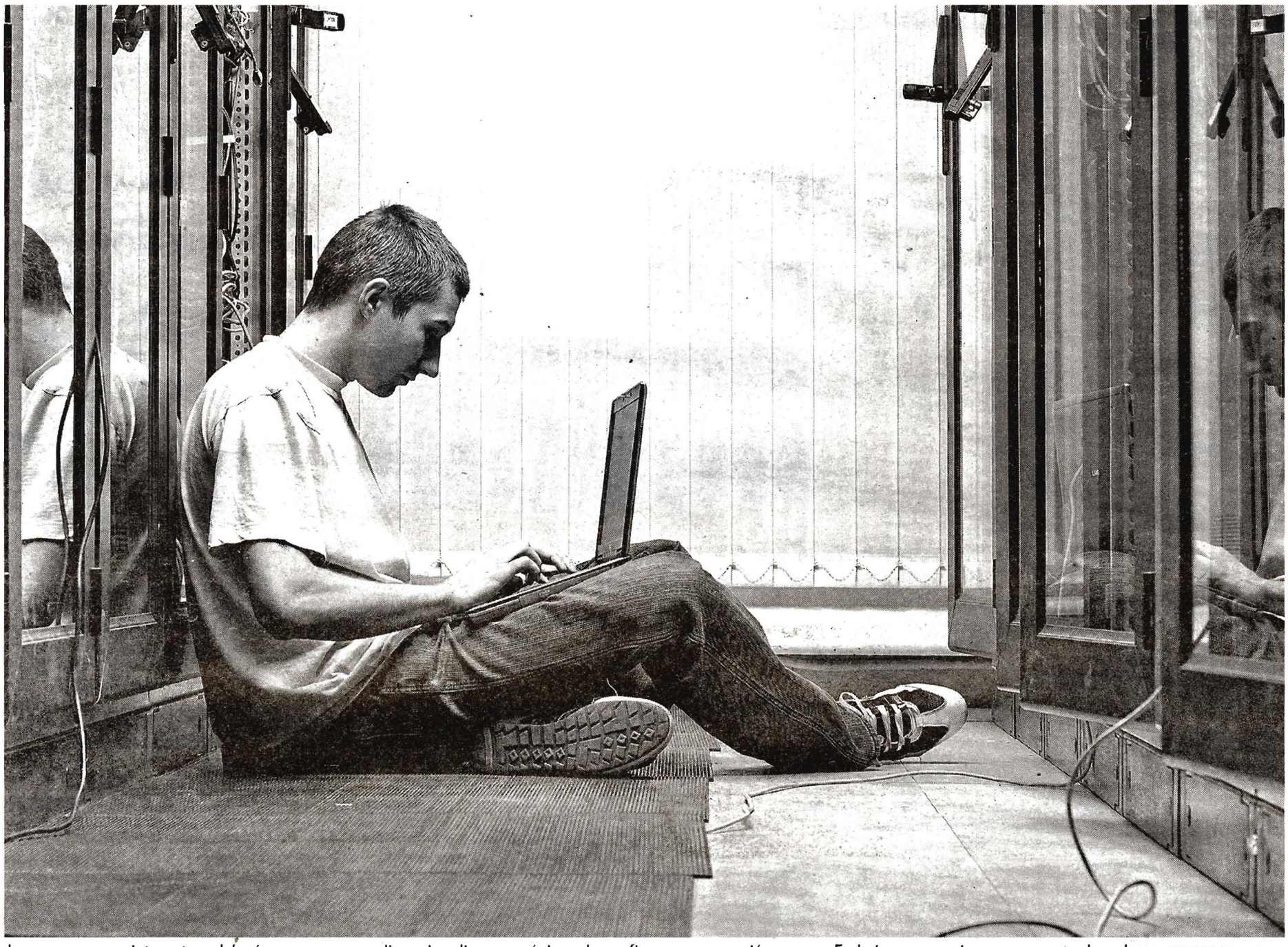
La escritora recuerda en esta entrevista que el genial escritor se enamoró de ella porque era «chiquita y le divertía», y que él era «como el conejo de 'Alicia en el país de las maravillas'.

12

'JANE EYRE' VUELVE AL CINE Y A LAS LIBRERÍAS

La reedición de la novela y su adaptación al cine abren el debate sobre la literatura de género. ¿Son las Hermanas Brontë para chicas? ¿Y Julio Verne para los chicos?

11



Las compras por internet no deberían suponer un peligro si realizan en páginas de confianza con conexión segura. En la imagen, un joven navega por la red. / SHUTTERSTOCK

CUANDO FACEBOOK DEJA HUELLA. Crece el acceso ilegal a datos personales por parte de algunas empresas

ANA LUZ DÍAZ

Era su primer día de trabajo pero llegó tarde. Cómo explicarle al jefe que había estado en la Policía para denuciar a un acosador cibernético. «¿Quién lo iba a creer?», lamenta Elena, que prefiere no mostrar su nombre real. Es el amargo inicio en el mundo laboral de una estudiante de Psicología de 20 años que vio cómo alguien robó sus claves y su perfil de facebook y lo utilizó para enviar insultos, amenazas y compartir archivos personales comprometedores a todos sus contactos. «No te atrevas a borrar esto o te atendrás a las consecuencias», amenazaba su acosador, treinta años mayor que ella, de su entorno familiar y con conocimientos avanzados de informática.

Cinco años después de los primeros indicios de acoso personal, esta joven estudiante ha perdido toda su intimidad también en la red. *«Tenía claro que por tu mentalidad adolescente me bloquearías de Facebook, pero recuerda que puedo entrar en cualquiera de tus cuentas siempre que quiera, en cualquiera»*, amenaza públicamente el acosador en el blog de la víctima.

Apropiarse de un perfil ajeno y compartir imágenes y videos no autorizados en la red son algunas de las principales denuncias que recibe la Agencia Española de Protección de Datos (AGPD). A diferencia del acoso y la violación intencionada de la seguridad de los equipos (por *hackers*), la mayoría de las actividades peligrosas para la privacidad en internet son actos cotidianos y no intencionados y que los usuarios, especialmente los jóvenes, realizan de forma bastante inconsciente: envíos autorizados de números de teléfono, etiquetado de fotos en el cajón de sastre indiscreto de las redes sociales o el uso de *software* pirata, entre otros.

Entre las malas prácticas habituales que se cometen en internet, el experto en seguridad de redes Pedro García Teodoro destaca la cesión libre de datos privados (edad, sexo, gustos, fotos...) en las redes sociales y la descarga de *software* ilegal.

«Las descargas gratuitas son muy sospechosas», reflexiona este catedrático de la Universidad de Granada y miembro del grupo de seguridad NESG (Network Engineering and Security Group). «Están potencialmente cargadas de software malicioso que puede infectar tu ordenador y utilizarlo para lanzar nuevos ataques y rastrear datos en la red», avisa. La solución, claro, es utilizar *software* siempre legal y no descuidar las actualizaciones del mismo. Otras maneras de contraer este *malware* son al abrir correo spam o acceder a enlaces infectados.

Incluso los gestos más *inocentes* pueden suponer una cesión de derechos de la intimidad a terceros. Es el caso de la invitación a jugar a Farmville, los bolos o las cartas, en Facebook. O a hacer un test de inteligencia y habilidades para competir con tus contactos. O mostrar en un mapa los lugares que has visitado en el mundo.

«Cada vez que te entretienes con un juego enlazado desde Facebook o participas en sus tests, estás firmando un nuevo contrato de adhesión», alertan desde la web de la Organización de Consumidores y Usuarios (OCU), que prosigue con este aviso: «Estas aplicaciones no forman parte de la red social. Son empresas independientes a las que el usuario ha permitido directamente ver su información personal».

Así, al darnos de alta en la aplicación (y no leer la letra pequeña –diminuta– de las condiciones de uso), nosotros mismos hemos aceptado gratuitamente que nuestros datos se esparzan por el espacio cibernético.

Con un clic, el individuo ha cruzado la barrera de la privacidad semi-controlada y su información personal ha pasado a manos de terceros, de los que desconoce las leyes que les rigen en cuanto a protección de datos. Si además se encarga de volver a compartir los datos con otros interesados, la cadena de información descontrolada se dispara por el mundo.

La Agencia Española de Protección de Datos advierte de las fronteras laxas de internet en materia jurídica. «Las empresas ubicadas en otros países –EEUU en el caso de muchas redes sociales– tienen una normativa de protección de datos no comparable con los estados europeos». En el caso de Tuenti, sin embargo, al estar sujeta a la jurisdicción española, tiene un mayor control sobre la privacidad de sus usuarios. «Además, no proporciona su información a ningún motor de búsqueda en red», recuerda la OCU, al contrario de lo que ocurre con Twitter y Facebook.

«La mayoría de la información que hay en internet es responsabilidad del propio cibernauta», asegura Genís Roca, de la consultora RocaSalvatella, especializada en el desarrollo de negocio mediante estrategias en la red.

«Un joven tiene dos maneras de dejar su huella en internet, consciente e inconscientemente», apunta, y esta información, según indica el experto, puede ser utilizada entre las empresas de publicidad y en las candidaturas para un puesto de trabajo. «Ante una decisión importante como es contratar a un nuevo empleado, las empresas no dudan en rastrear el perfil del candidato», afirma. Por eso es decisiva la imagen que internet proyecta de cada uno.

¿Qué pasa cuando la empresa accede a datos demasiado personales, a fotografías de ocio, y prejuzga al candidato? «Puede parecer injusto, pero si yo veo que alguien no ha tenido capacidad para gestionar la privacidad de su propia información, probablemente pensaré que no es capaz de gestionar la información de mi empresa», asevera Genís.

Las páginas que visitamos, los clics que hacemos en la publicidad, las búsquedas que realizamos... Todo deja una huella en nuestro historial. Aunque los jefes en potencia nunca van a acceder a estos mapas de nuesfra navegación, ciertas empresas sí se benefician de los rastros que el usuario deja inconscientemente en el ciberespacio: las relacionadas con la publicidad.

Hay rastreadores que enlazan cuentas de correo, teléfonos y datos geográficos, de sexo y de gustos para realizar estudios de perfiles y enviar publicidad a medida. «La banca, la telefonía, las agencias de viajes...han recopilado datos de sus clientes siempre en beneficio propio y para reorganizar sus estrategias de negocio», explica Genís.

Ahora, uniendo los datos que el usuario comparte libremente, más los estudios del comportamiento de un colectivo como los jóvenes universitarios, las empresas pueden realizar mejores estrategias de publicidad. En el caso, por ejemplo, de una tienda de ropa juvenil que quiera encontrar un emplazamiento ideal en la ciudad, expone Genís, podrían tener una fuente importante de datos sobre costumbres entre los jóvenes a la hora de comprar a través de los bancos; por el uso de sus tarjetas de crédito sabrían qué compran y en qué área lo hacen, cuánto gastan o con qué frecuencia. De ahí que sea importante conocer la política de cesión de contenidos de las empresas con las que tratamos.

«La publicidad sólo conoce información genérica sobre sexo, edad, ubicación geográfica e intereses», recuerda la OCU, y añade: «No te busca a ti, sino a muchos como tú». Estos actos, si recogen información publicada libremente, no son ilegales. El acceso ilegal a datos personales violando la seguridad del sistema es un delito punible, y para luchar contra el fraude y el ciberacoso la Policía Nacional cuenta con una Brigada de Investigación Tecnológica.

«Mi acosador consiguió apoderarse de toda mi información del ordenador, enviar fotos a mis contactos y falsear con comentarios de *me gusta* en páginas violentas o de conductas sexuales», recuerda Elena, que se ha cambiado recientemente de provincia para poner tierra física de por medio. «Pero salir de las redes sociales e internet no es la solución. Ahora al menos puedo controlar qué sigue escribiendo y defenderme», prosigue. Hoy quiere desaparecer, pero su pasado, el verdadero o el falseado, será muy difícil de eliminar. «Claro que te preocupa lo que pueda ver de ti el jefe. Lo que hayas colgado en la red con 18 años te puede arruinar la vida », lamenta. Y sentencia: «Las palabras se las lleva el viento. En internet no. Los jóvenes somos irresponsables con el uso de estas herramientas».

INDISCRECIÓN EN LAS REDES

En las redes están los amigos pero también los enemigos. La suplantación de la identidad, el robo de contraseñas y el acoso cibernético son los casos extremos de uso fraudulento (y en muchos casos, punible) de las redes sociales. El hecho de compartir datos como la edad, las fotos o las aficiones es un acto libre, aunque inconsciente en muchos casos, pues se olvida que internet es un espacio público sobre el que el usuario no tiene control final. «La simple creación de una cuenta hace que nuestra información básica aparezca directamente en los buscadores de internet», avisa la OCU. Esta información pública puede ser usada posteriormente, por ejemplo, para valorar a un candidato en una entrevista de trabajo. Además, desactivar una cuenta personal no garantiza la eliminación completa del perfil en la internet.

ENVIO MASIVO DE E-MAILS

Los virus y el software malicioso, conocido como 'malware', pueden introducirse en nuestros equipos a través de los correos electrónicos masivos, de los enlaces infectados o a través de la descarga de contenidos ilegales. Al enviar un mensaje por correo electrónico, la forma más segura para proteger la identidad de sus destinatarios es escribir los nombres de los contactos en la casilla de Copia Oculta (CCO). Además, se deben eliminar las direcciones de correo del cuerpo del mensaje. El 'spam' se nutre rincipalmente de los envíos masivos de correos para hacerse con bases de datos de cuentas activas, que se convertirán en nuevos objetivos de la basura cibernética. La solución es sencilla, pero los usuarios lo olvidan con frecuencia. Los mensajes en cadena son también la vía de trasmisión de mensajes fraudulentos.

DESCARGA ILEGAL DE 'SOFTWARE'

«El único ordenador que está seguro es el que no está conectado a la red», avisa Jorge Flores, de la asociación Pantallas Amigas. «Pero no hay que volverse paranoico», prosigue, «pues la mayoría de la información que existe en internet depende de nosotros».

En primer lugar, antes de culpar de 'spam' o fraudes a internet, hay que echar un ojo a nuestro equipo de conexión, ordenador o 'smartphone' para asegurarnos que está limpio de 'software' malicioso. «El uso de 'software' pirata es un buen caldo de cultivo para el 'malware'», explica el catedrático de la Universidad de Granada Pedro García Teodoro, experto en seguridad en redes. Los intrusos malintencionados rompen la seguridad de los ordenadores y teléfonos móviles, ponen en riesgo la privacidad de los datos y pueden rastrear contenidos desde otra IP.

LOS JUEGOS Y TESTS 'ON LINE'

Los enlaces a juegos o a tests de inteligencia y habilidades desde Facebook suponen un nuevo contrato de adhesión con la empresa externa. Si se accede a estas aplicaciones, se está aceptando compartir los datos públicos con los responsables del juego o el test. La Organización de Consumidores y Usuarios (OCU) advierte de que estas empresas son independientes de la red social y es el usuario el que le permite el acceso directo a los datos propios.

Es bastante improbable que el cibernauta conozca, a partir de ahí, el uso que se haga de la información personal. Asimismo, la Agencia Española de Protección de Datos (AEPD) alerta de las diferencias de legislación en materia de protección de datos que existen entre países extranjeros, como EEUU, y el mayor nivel de protección en la Unión Europea.

COMPRAS CON GARANTÍA

El uso de una tarjeta de crédito en internet es igual de seguro que cuando se utiliza en un restaurante o una tienda de ropa, ya que la validación y la realización efectiva del pago es el mismo en ambos casos. Para garantizar la confidencialidad en la transferencia de datos en internet, se usa el protocolo de seguridad SSL ('Secure Sockets Layer'). Dos señales básicas de que se está accediendo a una página protegida es que, en la barra de direcciones, la url comienza con https:// (con la letra ese al final) y en la esquina inferior derecha aparece un candado cerrado. Aún así, ninguna operación de compra está libre de sufrir un fraude, por lo que la OCU invita a recelar de los precios anormalmente bajos y huir de los sitios que muestran faltas de ortografía o que sólo ofrezcan un móvil como única identificación.

DEJAR HUELLA SIN SABERLO

En internet hay dos tipos de datos personales, los que publicamos, libremente, y los que generamos incoscientemente. Entre los segundos se encuentra el rastro que dejamos a nuestro paso por el ciberespacio. Las páginas que visitamos, las descargas que hacemos o las búsquedas que realizamos se quedan grabadas en las 'cookies' de nuestro ordenador y se convierten en una fuente de información para posibles 'lanzadores' de publicidad adaptados a nuestro perfil. Unidas a la información que publicamos libremente, por ejemplo en una red social, las empresas asociadas a publicidad logran fácilmente situar al usuario dentro de un colectivo propenso a recibir anuncios. En las redes sociales, las empresas externas pueden acceder con más facilidad a los gustos de los usuarios.