Apps y seguridad

AVACU
asociación valenciana de consumidores y usuarios


AVACU
asociación valenciana
de consumidores
y usuarios

Un smartphone es un teléfono móvil con pantalla táctil que nos permite realizar tareas más avanzadas que un teléfono convencional: acceder a internet, gestionar cuentas de correo electrónico, chatear, hacer fotos o vídeos, acceder a redes sociales o instalar juegos y aplicaciones como si de un ordenador se tratara. Desde la llegada de los primeros teléfonos móviles, que apenas nos permitían realizar llamadas y enviar SMS, la aparición de los smartphones ha supuesto una verdadera revolución en el sector y el grado de aceptación de este dispositivo como un elemento fundamental de nuestras vidas es más que evidente. Actualmente el alcance del móvil es mayor que nunca, afectando a nuestro día a día, a nuestro comportamiento y a nuestra forma de comunicarnos.

A esto hay que añadirle la aparición de tecnologías que nos permiten mayores velocidades de conexión para el acceso a contenidos, descargas, chat, etc. y que han propiciado un aumento exponencial en el número de servicios y aplicaciones de ocio, productividad, comunicación o social que se presentan en el mercado.

En relación a esto último, el mercado de las ***apps*** ha crecido enormemente en los últimos años, en paralelo al de los smartphones. Cada vez nos encontramos más aplicaciones que nos permiten hacer casi cualquier cosa, inimaginable antes en un teléfono móvil, y, en muchos casos, nos han permitido sustituir el PC. ¿Para qué voy a encender el ordenador para leer el correo si puedo hacerlo desde el móvil o la tablet?

Se podría decir que un smartphone es el equivalente a llevar un PC en la mano. Esta afirmación supone una ventaja evidente: gracias a los smartphones y las ***apps*** se puede hacer cualquier cosa en cualquier lugar. Sin embargo, este crecimiento ha venido acompañado de la aparición de una gran cantidad de software malicioso, ataques, cibercriminales y demás delitos informáticos asociados cada vez más al mundo móvil. Así, todas las vulnerabilidades por las que puede verse afectado un ordenador se aplican también a los smartphones. Por tanto, debemos adoptar una serie de precauciones de seguridad tal y como lo hacemos (o deberíamos) con nuestros ordenadores. A continuación vamos a profundizar en el mundo de las ***apps***, la privacidad y seguridad en nuestros móviles e intentar responder a muchas preguntas que los usuarios *móviles* nos hemos hecho alguna vez.

(6) **Apps para móviles: ¿qué son y cómo funcionan?**

¿Son seguras las apps?
¿Qué riesgos conllevan los permisos de las apps?
¿Qué ocurre cuando desinstalamos una app?

(12) **Tipos de apps**

De mensajería instantánea
De banca electrónica

(18) **Amenazas a las que estamos expuestos**

Qué hacer si nuestro móvil está infectado

(20) **Consejos de seguridad y privacidad que debes tener en cuenta**

Apps para móviles: ¿qué son y cómo funcionan?

Una *app* es una aplicación informática diseñada para móviles o tablets que realiza una serie de funciones para la que ha sido programada. Existen *apps* para realizar cualquier tarea cotidiana, chatear, acceder a redes sociales, juegos, catálogos, compras, información de productos, viajes, guías, aplicaciones corporativas para su uso en una empresa, etc.

Las aplicaciones o ***apps*** pueden ser desarrolladas por empresas o particulares, pueden ser gratuitas o de pago, pueden ser utilizadas en uno o varios sistemas operativos (como Android, iOS, Windows Phone, Blackberry...). Se descargan e instalan en los smartphones a través de las tiendas de aplicaciones de las principales plataformas y, muchas de ellas, hacen uso de recursos del teléfono, como la agenda, fotos, tarjeta de memoria o localización GPS.

Las ventajas que ofrecen las ***apps*** son múltiples: chatear o intercambiar fotos y videos con familiares y amigos sin coste extra, acceder a las redes sociales o a internet desde cualquier lugar, jugar, acceder a las cuentas bancarias, realizar pagos o compras, etc.

De lo que no todo el mundo es consciente es que, detrás del mundo de las ***apps***, nuestra privacidad puede verse comprometida y somos vulnerables ante posibles ataques de seguridad, tal y como ocurre con un ordenador de casa o del trabajo.

¿Son seguras las *apps*?

La respuesta a esta pregunta es sencilla: depende. Y depende fundamentalmente de dos factores: si la aplicación fue creada con fines maliciosos y el uso que hagan los usuarios del smartphone. Las aplicaciones maliciosas (malware) son aquellas que están creadas para engañar al usuario y obtener información privada o credenciales de acceso con el fin de obtener un beneficio económico.

Respecto a lo segundo, muchas veces los usuarios no somos conscientes de que un smartphone está conectado a una red global como es internet y que por ella viajan constantemente nuestros datos personales, fotos, contraseñas u otra información privada. Y, además, viaja con nuestro consentimiento, por lo que debemos ser conscientes de qué estamos compartiendo o publicando y con quién.

Podría llevar días o semanas analizar profundamente cuan seguras son las *apps* que se instalan habitualmente. Se han hecho varios análisis en los últimos años y la conclusión a la que se llega es que las *apps* no son 100% seguras, ya que no implementan todos los mecanismos de seguridad que deberían.

En algunos casos, no se incluyen mecanismos de encriptación y cifrado, es decir, mecanismos que aseguren que la información que viaja por internet o se almacena en nuestro teléfono no viaja "abierta", sino codificada para evitar que un extraño pueda leerla.

En otros casos existen vulnerabilidades de seguridad en la parte del servidor de un determinado servicio, como una tienda, red social o chat. Con todo, hay que ser conscientes de que el smartphone y las *apps* están conectados y, por tanto, no se puede garantizar al 100% la seguridad de los datos. Pensemos, pues, qué parte de nuestra vida queremos compartir y qué parte no.

¿Qué riesgos conllevan los permisos de las *apps*?

Cuando se instala una *app*, el primer paso es la validación de los permisos de acceso. En este paso inicial se detalla cada uno de los recursos a los que la aplicación necesita acceder, teniendo en cuenta las funciones que ofrece: por ejemplo, una aplicación de mensajería instantánea solicita habitualmente permiso para acceder a la memoria para el acceso a nuestras fotos, al GPS para obtener nuestra localización, a nuestra agenda de contactos, a la cámara, al WiFi, etc. En el momento en el que aceptamos esta solicitud, damos vía libre a la aplicación para manejar todos esos recursos.

Algunos de los permisos más habituales y sus posibles usos fraudulentos son:

Agenda de contactos y registro de llamadas	permite acceder a la información de teléfonos, mails... Utilizado ilícitamente podría ser empleado para recibir SMS o mails fraudulentos que conlleven una estafa telefónica o la descarga de una app maliciosa.
Listado de SMS	podría permitir el envío de SMS maliciosos por parte de un cibercriminal para suscribir al usuario a servicios premium.
Fotos, videos o audios	podrían ser copiados y ser utilizados para extorsiones o contrabando ilegal de material audiovisual.
Datos de localización (GPS)	estos datos podrían permitir a un tercero comerciar con los hábitos de una persona, conocer su localización y perpetrar robos o secuestros.
Teclado	algunas aplicaciones de teclado utilizan las pulsaciones del usuario para rastrear contraseñas o tarjetas de crédito.
Almacenamiento	el acceso a la tarjeta SD o al almacenamiento interno del teléfono puede permitir a terceros instalar software malicioso o acceder a documentos privados o confidenciales.

En muchas ocasiones el uso de datos privados o el acceso a recursos del teléfono suele hacerse para fines no delictivos. Algunas aplicaciones toman datos de uso, localización u otros datos del teléfono para fines comerciales. Con esta información se obtienen una serie de datos estadísticos que son vendidos a empresas de publicidad, lo que se traduce, entre otras cosas, en banners publicitarios a medida de los gustos o hábitos de los usuarios.

Aunque pueda parecer extraño, es muy habitual: una empresa referencia como Google conoce en todo momento nuestra ubicación y nuestros hábitos de consumo. En cualquier caso, no se trata de un uso delictivo de nuestro teléfono, aunque podamos sentirnos vulnerados a nivel de privacidad.

Lejos de ser alarmistas, debemos ser conscientes de lo que aceptamos y es muy recomendable leer bien los permisos de acceso que se presentan antes de la instalación.

Dicho así puede sonar muy intrusivo, pero no nos alarmemos. Las ***apps*** más populares no suelen abusar del usuario. Lo que los usuarios aceptamos son categorías de permisos, pero dentro de cada categoría hay una gran cantidad de opciones, muchas de ellas desconocidas para el usuario, que la ***app*** puede cambiar a su antojo sin avisar. Por ejemplo, dar acceso a la categoría SMS puede significar poder enviar o recibir mensajes, pero también leer o incluso editar los SMS del teléfono.

Muchas aplicaciones hacen uso de más recursos de los estrictamente necesarios. Algunas aplicaciones de transporte público piden, por ejemplo, acceso al almacenamiento, cuando lo único que hacen es ofrecer a qué hora va a llegar el autobús. *¿Es necesario?* Probablemente no.

¿Qué ocurre cuando desinstalamos una *app*?

Cuando los usuarios detectan un peor funcionamiento de sus smartphones o tablets, o bien tienen ciertas sospechas de tener un software malicioso instalado, el primer acto reflejo es desinstalar esa *app* sospechosa. Si bien es cierto que en ese punto el ataque puede haberse producido ya, desinstalar la *app* sospechosa es el primer paso a seguir.

Pero, ¿es suficiente? Posiblemente no. Al desinstalar una *app*, el sistema la elimina de los directorios donde se instala, liberando además memoria del teléfono. Sin embargo, puede haber software malicioso que, en el proceso de instalación, haya creado ficheros, gusanos, troyanos o demás archivos sospechosos en otras ubicaciones del teléfono, como por ejemplo, alguna carpeta en la tarjeta SD. Es por ello que es conveniente revisar todas las carpetas del teléfono y eliminar todo fichero que parezca sospechoso.

Además, aun no siendo maliciosos, al desinstalar una *app* pueden quedar en la memoria restos de ficheros o carpetas basura que no hacen más que ralentizar el sistema y hacer que el teléfono vaya menos fluido. Por ello, puede ser recomendable hacer una limpieza cada cierto tiempo o incluso restablecer los datos de fábrica.

Para ello, existen herramientas de limpieza que eliminan esos "restos" de las aplicaciones desinstaladas, algunos de los cuales podrían ser maliciosos. Además, algunas de estas herramientas limpian el historial del navegador, cachés con cientos de megas de datos inútiles de aplicaciones desinstaladas, miniaturas de imágenes, etc., que no hacen más que estorbar y ocupar espacio en la memoria del dispositivo.

Tipos de *Apps*

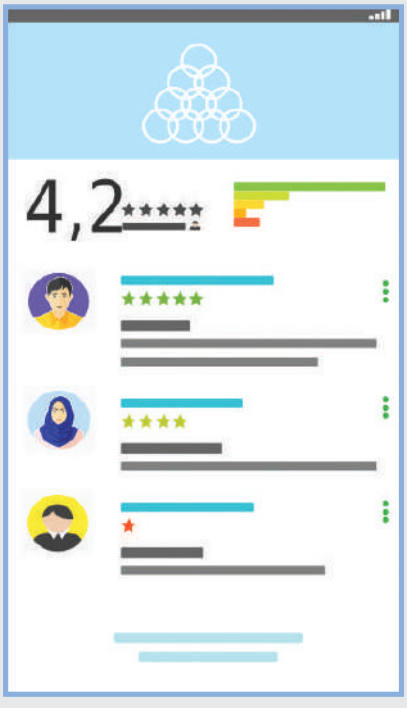
Las *apps* son desarrolladas por empresas o particulares, pueden ser gratuitas o de pago, ser utilizadas en uno o varios sistemas operativos (como Android, iOS, Windows Phone, Blackberry…), se descargan e instalan en los smartphones a través de las tiendas de aplicaciones de las principales plataformas y, muchas de ellas, hacen uso de recursos del teléfono, como la agenda, fotos, tarjeta de memoria o localización GPS.

Las ventajas que ofrecen las *apps* son múltiples: chatear o intercambiar fotos y videos con familiares y amigos sin coste extra, acceder a las redes sociales o a internet desde cualquier lugar, jugar, acceder a las cuentas bancarias, realizar pagos o compras, etc.

De lo que no todo el mundo es consciente es que, detrás del mundo de las *apps*, nuestra privacidad puede verse comprometida y somos vulnerables ante posibles ataques de seguridad, tal y como ocurre con un ordenador de casa o del trabajo.

Apps de pago: ¿más seguras?

Existen, en las tiendas, aplicaciones de pago o versiones de pago de muchas aplicaciones que, en su versión más sencilla, son gratuitas. En otras ocasiones, las aplicaciones son gratuitas en el momento de su descarga, pero luego ofrecen la posibilidad de habilitar características premium de pago, lo que se conoce como compras "*in-App*".



La mayoría de estas aplicaciones ofrecen ventajas en funcionalidad respecto a otras:

- Eliminación de publicidad que aparece en su versión gratuita.
- Más opciones o características más avanzadas.
- Contenidos premium o contenidos con copyright.
- Uso ilimitado, mientras que su versión gratuita está limitada en tiempo.
- Mayor calidad, seguridad y mejor resultado final.

Esta última afirmación, aunque no siempre es cierta, sí se cumple en un buen porcentaje. Una aplicación de pago no tiene porqué ser más segura que una gratuita, sin embargo, hay más probabilidades de que lo sea.

Apps de mensajería instantánea

Las *apps* de mensajería instantánea han supuesto una auténtica revolución en los últimos años. Ya ha quedado atrás esa época en la que nos comunicábamos, además de mediante las llamadas de voz, con SMS o mensajes de texto. Aunque en muchos países ambos servicios se utilizan casi a la par, en España la mensajería instantánea dobla en uso al envío de esos SMS.

De hecho, tras las llamadas de voz, la mensajería instantánea es el segundo servicio más utilizado en los smartphones de los españoles. Además, el uso de la mensajería instantánea no se limita a una única *app*. Más de un 50% de los españoles afirma utilizar al menos dos *apps* distintas para comunicarse con familiares, amigos o colegas de trabajo.

Este crecimiento exponencial de estas *apps* ha venido dado principalmente por factores como:

- Mayor comodidad e instantaneidad
- Más económico que los SMS
- Más fácil de usar que los SMS
- Permite el envío de fotos, videos o audios además del texto
- Permite conversaciones grupales
- Gran difusión en el público más joven

Por tanto, se puede afirmar que, dentro de las *apps*, las de mensajería instantánea se han convertido en parte de nuestras vidas. Por todo ello, debemos prestar especial atención a ciertas consideraciones de seguridad y privacidad en relación a este grupo de aplicaciones. Si pensamos en *apps* de mensajería, la primera que nos viene a la cabeza es WhatsApp. Es fácil entenderlo: según el *V Informe de las apps* en España (septiembre de 2014), el 98,5% de los usuarios utiliza WhatsApp. Sin embargo existen otras alternativas más que válidas, cuyo uso en otros países está más extendido.

Tras los escándalos de filtraciones de datos privados de empresas, celebrities... muchas *apps*, y en especial las de mensajería instantánea, han puesto el foco en las cuestiones de seguridad, destacando este aspecto como un punto fuerte frente a sus competidores. Sin embargo, sigue surgiendo la duda de cuan seguras son estas *apps*. Por todo ello, las *apps* de mensajería instantánea, no siendo una amenaza para nuestra seguridad y privacidad, tienen que considerarse seguras sólo relativamente, por lo que las precauciones en esta materia son siempre más que recomendables.

Las *apps* de mensajería instantánea más comunes son:

- **WhatsApp**: servicio de mensajería por excelencia, con más de 800 millones de usuarios.
- **Line**: alternativa más popular, primera en ofrecer llamadas de voz.
- **Skype**: ofrece videoconferencia, que es por lo que más se la conoce.
- **Telegram**: los mensajes se autodestruyen pasado un tiempo, por lo que apuesta fuertemente por la privacidad.
- **Facebook Messenger**: destaca por su sincronización con la red social más conocida.
- **Viber**: su punto fuerte son las llamadas de voz y la videoconferencia.
- **Snapchat**: elimina los mensajes pasado un cierto tiempo, en el móvil que lo envía y en el que lo recibe.
- **Spotbros**: alternativa española que pone el foco en la privacidad, por ejemplo, no permitiendo envío o recepción de mensajes de números desconocidos.
- **Wechat**: una buena alternativa, muy consolidada en otros países, con 600 millones de usuarios.

Apps de banca electrónica

Otras aplicaciones en auge en los últimos tiempos son las de banca electrónica. Muchas personas utilizan hoy en día las aplicaciones de su banco para transferir dinero, pagar recibos o consultar las finanzas. Las *apps* de banca electrónica permiten hacer casi cualquier operación que hasta ahora se hacía a través de un navegador web. Es por eso que cada vez más bancos ofrecen aplicaciones para poder realizar estas operaciones a cualquier hora y en cualquier lugar.

Sin embargo, todavía hay muchas personas reacias al uso de este tipo de aplicaciones. El principal motivo es la seguridad y es que, si bien la falta de seguridad no nos importa demasiado cuando se trata de *apps* de mensajería instantánea o redes sociales, donde compartimos datos personales y de nuestra vida cotidiana, cuando se trata de dinero, la percepción de la seguridad cambia bastante.

Muchos bancos y algunos expertos en materia de seguridad señalan que el uso de *apps* bancarias es más seguro que la banca electrónica a través del PC mediante un navegador web. Aunque esta afirmación es correcta, también lo son algunos datos de estudios realizados que revelan que la seguridad de este tipo de *apps* es más que relativa y depende mucho de la inversión que la entidad bancaria haga en materia de seguridad.

¿Hay peligro real? Existen estudios que revelan que el 90% de las *apps* bancarias presenta algún tipo de vulnerabilidad. Si bien es cierto que esa cifra puede ser exagerada, sobre todo porque las entidades bancarias invierten cada vez en mejorar este aspecto, debemos prestar especial atención a ciertas precauciones en el uso de este tipo de *apps* y así poder utilizarlas con cierta tranquilidad.

Expertos en la materia han hallado diversas vulnerabilidades en las *apps* de banca electrónica, como por ejemplo no cifrar el 100% de las transacciones con SSL (protocolo de encriptación que hace ilegible los datos enviados por la red), generar ficheros en el teléfono con datos personales y de historial de transacciones sin cifrar o vulnerabilidades frente ataques de phishing, que permiten por ejemplo obtener a un tercero las credenciales solicitando al usuario de forma fraudulenta que las vuelva a insertar porque la sesión ha caducado.

Con este tipo de medidas podemos hacer uso de este tipo de aplicaciones sin problemas. Como se ve, se trata de medidas que podemos aplicar a cualquier tipo de *app*, pero son más críticas cuando se trata de proteger nuestro dinero.

- Instalar la *app* oficial: lo más recomendable es asegurarse de que el banco certifica la seguridad de la *app* y la publicita en sus oficinas y en su web oficial, donde se suele indicar la forma correcta de descargar e instalar la *app*.
- Mantener actualizada la *app* y el sistema operativo del teléfono.
- Instalar un antivirus y realizar con frecuencia chequeos antimalware.
- Evitar dejar el teléfono desbloqueado y configurar una clave de bloqueo.
- No conectarse a redes wifi no seguras.
- No almacenar datos bancarios en el teléfono, por ejemplo en blocs de notas, mails o mensajes.

Amenazas a las que estamos expuestos

El malware ha existido siempre en ordenadores personales, pero en los últimos años ha crecido en el mundo de los smartphones a un ritmo vertiginoso. Los cibercriminales demuestran cada vez más interés en este tipo de dispositivos por la gran cantidad de usuarios que los utilizan y porque cada vez se realizan más tareas con los móviles que antes se realizaban en el PC. Aunque pueden afectar a todas las plataformas, Android quizá sea más vulnerable debido a su política de publicación de aplicaciones en Google Play, más flexible que por ejemplo la de Apple, que revisa una a una las aplicaciones antes de permitir su publicación.

¿Qué hacer si nuestro móvil está infectado?

Muchas veces la presencia de software malicioso en nuestros smartphone es evidente, pero en otras ocasiones se hace complicado detectarlo. Estos son algunos síntomas que puede presentar un móvil ante la presencia de ***malware***:

• **Facturas más elevadas de lo habitual**: por la suscripción a servicios *Premium*, que pueden incrementar la factura considerablemente.

• **Consumo excesivo en la tarifa de datos**: en ocasiones el ***malware*** consume la tarifa de datos contratada o fuerza conexiones a determinadas webs, a anuncios o a descargas de ficheros.

• **Mal funcionamiento del terminal**.

• **Aparición de aplicaciones no descargadas por el usuario** en el teléfono o de anuncios no deseados.

El término malware (del inglés *mal*icious soft**ware**), código maligno o software malintencionado, es un tipo de software que ha sido diseñado para infiltrarse en un ordenador o smartphone y dañarlo u obtener información sensible sin el consentimiento del usuario. Incluye troyanos, gusanos, virus, spyware, phishing, adware, etc., según el daño causado en el equipo.

En muchas ocasiones el malware se introduce en un smartphone por la instalación de *apps* de dudosa confianza. Por ello, el primer paso es eliminar toda aquella aplicación que no pertenezca a markets oficiales. Si aun así el problema persiste, la mejor solución es instalar un buen antivirus y realizar un escaneo. Como última opción, lo mejor es restablecer el smartphone a ajustes de fábrica.

Consejos de seguridad y privacidad que debes tener en cuenta

Después de todo lo comentado en apartados anteriores, queda claro que el móvil, al igual que el PC, nos ha facilitado la vida enormemente y nos permite hacer casi cualquier tarea cotidiana. Pero, por ello, debemos tener ciertas precauciones en materia de seguridad, ya que estos dispositivos no son 100% seguros y los cibercriminales se esfuerzan constantemente en buscar ese agujero de seguridad que comprometa nuestra privacidad.

☑ **No instales aplicaciones que no provengan de fuentes oficiales**: no es nada recomendable instalar ***apps*** de markets no oficiales o de sitios web de dudosa reputación.

☑ **Instala sólo aplicaciones confiables y de desarrolladores reputados**: aún haciendo uso de los markets oficiales, los cibercriminales pueden ser capaces de publicar aplicaciones ilegítimas de forma encubierta.

☑ **Cuidado con los emails**: no te descargues ficheros adjuntos a emails de orígenes o remitentes desconocidos y no accedas a webs que solicitan insertar credenciales si el email es de dudosa procedencia.

☑ **Cuidado con los timos por SMS o *apps* de mensajería**: no pulses sobre mensajes dudosos, cuyo único objetivo es hacernos consumir servicios *Premium* de forma desmedida.

☑ **Revisa minuciosamente los permisos solicitados** por las ***apps***, rechazando aquellas que soliciten permisos excesivos.

☑ Asegúrate de que las ***apps*** que ofrecen determinado servicio **cumplen con la ley de protección de datos de carácter personal**, y revisa los términos y condiciones.

☑ **No instales *apps* innecesarias** y desinstala aquellas que no se utilicen.

☑ **Evita la conexión a ordenadores públicos o desconocidos**, que podrían contener un virus e infectar nuestro dispositivo.

☑ **Evita versiones no oficiales del sistema operativo**, que pueden contener agujeros de seguridad.

☑ **Evita redes wifi gratuitas y abiertas**: muchos cibercriminales montan redes wifi abiertas en sitios públicos para enganchar a los usuarios y espiar sus dispositivos, pudiendo incluso leer sus usuarios y contraseñas de *emails*, redes sociales o banca online. No olvides desconectar el wifi y el GPS cuando no los uses.

☑ **Evita la conexión a puntos de recarga públicos**: algunos cibercriminales utilizan este servicio de algunos centros comerciales para conectarse libremente al teléfono, acceder a información privada o instalar un malware.

☑ **Instala un antivirus** y restaura el dispositivo a valores de fábrica de vez en cuando.

☑ Usa el **bloqueo de la pantalla**, pero cuidado: algunos terminales ofrecen desbloqueo por huella dactilar y, aunque este método puede parecer muy seguro a priori, los cibercriminales ya disponen de métodos para clonar el patrón de la huella; y nuestra huella no cambia nunca, pero una contraseña la podemos cambiar las veces que queramos.

☑ En este aspecto, **usa contraseñas no demasiado sencillas y cámbialas con asiduidad**.

☑ **Cuidado con lo que compartes** por mensajería instantánea o al subirlo a la *nube*: se trata de servicios seguros pero no infalibles. No subas ni compartas lo que no quieras que llegue a manos de otros bajo ningún concepto.

Por todo ello, es muy recomendable instalar sólo:

Descargar una aplicación y aceptar sus condiciones de uso no priva a los usuarios de sus derechos. Ante cualquier duda, consulta con una asociación de consumidores que te pueda asesorar.

Asociación Valenciana de Consumidores y Usuarios:

C/ Dr. Sumsi 28, bajo. 46005 **VALENCIA**

C/ Juan Bta. Lafora, 3, entrepl. 03002 **ALICANTE**

C/ Sanahuja 68, entresuelo A. 12004 **CASTELLÓN**

e-mail: avacu@avacu.es
http://www.avacu.es

1ª edición. Año 2017

AVACU agradece la colaboración de D. Juan Antonio Díaz Segura, CEO & Product Manager Near2com Technologies S.L., en la elaboración de los contenidos de esta guía.


AVACU
asociación valenciana
de consumidores
y usuarios