GUÍA PRÁCTICA

Uso y experiencia en redes sociales, la publicidad digital, la información y compra online

ADICAE
Asociación de Usuarios de Bancos, Cajas y Seguros

Edita:
ADICAE, Asociación de Usuarios de Bancos, Cajas y Seguros.
Servicios Centrales
C/ Gavín 12, local. 50001 Zaragoza.

Depósito legal: Z 2012-2019

Con el apoyo del Ministerio de Sanidad, Servicios Sociales e Igualdad.
Su contenido es responsabilidad exclusiva de la Asociación.

1. Introducción a las redes sociales y las herramientas digitales de información p.4

2. Retos de los consumidores en la información, interacción y compras por Internet p.6

3. La protección del consumidor ante la publicidad digital p.11

4. El buen uso de las aplicaciones móviles p.13

Introducción a las redes sociales y las herramientas digitales de información

Las redes sociales son ya una realidad que no podemos obviar. Las ventajas son muchas pero también hay muchos inconvenientes que debemos tratar de paliar con ayuda de las configuraciones de privacidad que ofrece cada plataforma y algo de sentido común. Las principales redes son:

Twitter:

Es una de las favoritas a cualquier edad. Se puede utilizar con un alter ego o pseudónimo e incluso hacerlo de manera privada, aunque de esta forma no verá nadie los tuits (comentarios) y la red pierde su sentido. Además, contiene pocos anuncios ya que su precio es elevado y las empresas optan por otras redes, sin embargo, puedes estar expuesto a mensajes de los perfiles de las empresas que disfrazan de comunicación lo que es claramente publicidad.

Facebook:

Nace con la finalidad de reencontrar amistades de la niñez y recuperar el contacto. Su configuración de privacidad permite que no se muestre tu nombre, tu foto e impide que se te busque por email o número de teléfono. Además puedes hacer tus comentarios privados e incluso ocultar información para algunos contactos de manera selectiva. Ofrece múltiples herramientas para evitar que tus datos personales estén expuestos. Sin embargo, la compañía los puede utilizar para segmentar los anuncios que te impactan dentro de la plataforma.

Instagram:

Es la red favorita por los nacidos entre finales de los 80 y los años 90. Se puede hacer la cuenta privada pero, como ocurre con Facebook (empresa propietaria de Instagram), la compañía puede ver tus datos y emplearlos para mejorar los impactos. La recomendación es introducir el mínimo de datos personales posibles.

TikTok:

La red de moda entre los adolescentes. Fue la app más descargada en España durante 2018 y la ventaja con la que juegan sus usuarios es que los mayores de 30 no le ven el interés. En esta red la celeridad y la creatividad mandan pero los riesgos son los mismos. Lo mejor, maximizar el sentido común y desconfiar de todos los anuncios que podamos ver en ella.

Algunos consejos que pueden resultar muy útiles a la hora de iniciar en las redes sociales es tener **un correo sólo para el registro en redes sociales, ajeno al que utilicemos para cuestiones laborales, bancarias y demás asuntos personales. También debemos omitir algunos datos al registrarnos, como pueden ser el DNI, la dirección de nuestra casa, la fecha de nacimiento o nuestro nombre completo. Desde hace algunos años, Facebook no admite todo tipo de pseudónimos pero sí nombres que aparenten ser reales.**

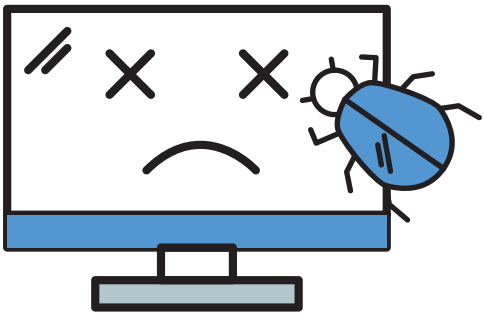
Retos de los consumidores en la información, interacción y compras por Internet

Como usuarios de herramientas digitales, debemos ser precavidos porque hay miles de estafadores que pretenden ganar dinero y obtener datos personales. Estas son los riesgos y fraudes más frecuentes:

» **Phising:** es un modo de engañar al usuario haciéndole creer que está en una web auténtica y segura. El objetivo es robar información privada (como contraseñas o datos bancarios) o, directamente, dinero.

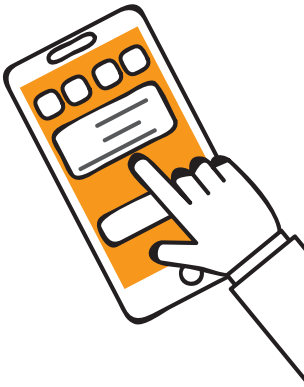
» **Pharming:** consiste en manipular la dirección IP (que se crean al acceder a cualquier web) con un código malicioso y cuando el usuario cree que está accediendo a la web de su banco en internet, realmente está accediendo a la IP de la página falsa. Tras esto, el objetivo es el mismo que en el *phising*, obtener contraseñas y datos bancarios.

» **Formjacking:** los estafadores inyectan un software malicioso en los medios de pago de los comercios online, copiando los datos personales y bancarios del comprador, mandando dichos datos al comercio y a los delincuentes.



» **Estafas sentimentales y de caridad:** una persona comienza una relación con otro usuario para pedirle dinero. También existe la vertiente que apela a la caridad o solidaridad para una ONG inexistente.

» **Ofertas de empleo falsas:** son ofertas de empleo con muy buenas condiciones, casi increíbles, pero que te piden dinero para tramitar papeles o enviar documentación antes de comenzar el falso trabajo.



» **Oportunidades de negocio:** es similar a la estafa anterior. En este caso te ofrecen invertir en productos o una empresa con enormes posibilidades de crecimiento, para lo cual, como no, te piden dinero para trámites o documentación.

» **Fraudes relacionados con la tarjeta de crédito:** los ciberdelincuentes crean sitios web, aparentando ser auténticos, con falsos descuentos y promociones que se compran mediante tarjetas de crédito.

Malas prácticas de las redes sociales

Como en la vida real, las redes sociales pueden servir para conocer gente, crear movimientos sociales, reencontrarse con viejas amistades o, simplemente, buscar información o datos, pero no por ello está libre de peligros.

Por ello, es importante conocer los riesgos y amenazas que tienen las redes sociales, pero también hay que tener en cuenta las herramientas que existen para evitarlos.

A continuación veremos los principales riesgos a los que nos arriesgamos por ser usuarios de las redes sociales.

» **Ciberacoso (Ciberbullying):** muchos acosadores aprovechan el anonimato y la sensación de impunidad que otorgan las redes sociales para atacar virtualmente a la gente. Uno de los principales problemas es que afecta a todas las edades, incluyendo menores, a los cuales pretenden humillar, avergonzar o difundir rumores sobre ellos.

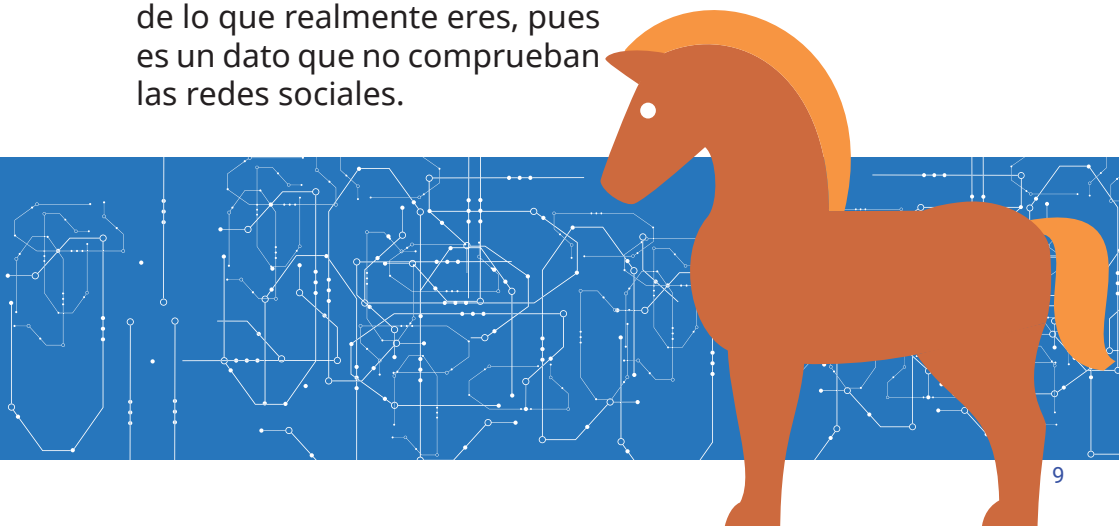
» **Fake news:** son noticias falsas que se difunden por las redes sociales que se han vuelto muy comunes los últimos años. Su finalidad es, simplemente, desinformar e intentar manipular a los usuarios de las redes sociales.

» **Uso indebido de tus fotografías:** cuando subes una fotografía a tus redes sociales, si no configuras correctamente tu cuenta, cualquiera podría verla. Además, en la mayoría de acuerdos que aceptas para poder interactuar en las redes sociales, indican que cualquier contenido que subas, pasa a ser propiedad de la red social.

» **Suplantación de identidad:** en las redes sociales cualquier persona puede ponerse tu nombre y tu foto de perfil, haciéndose pasar por ti. En ocasiones, esto se utiliza para actuar como la persona usurpada, realizando acciones maliciosas, como publicar mensajes injuriosos o contenidos inapropiados.

» **Malware:** es cualquier tipo de software malicioso que intenta infectar tu *smartphone* u *ordenador.* Las redes sociales son uno de los lugares más vulnerables con respecto al *malware. P*ueden, desde mandarte *spam* hasta conseguir tus datos personales.

» **Peligro para los menores:** como hemos visto anteriormente, los menores corren ciertos peligros en las redes sociales. Si bien, la mayoría de redes sociales piden una edad mínima para participar, basta con indicar que eres mayor de lo que realmente eres, pues es un dato que no comprueban las redes sociales.



Consejos para el buen uso de las redes sociales

A pesar de los riesgos que hemos enumerado anteriormente, hay una serie de herramientas y recomendaciones a las que debemos dar uso para poder utilizar las redes sociales de la forma más segura posible.

Infórmate:
Conoce las políticas y términos de uso de las distintas redes sociales a las que subes imágenes o texto, para saber qué derechos tienen sobre dicho contenido.
Configura tu cuenta:
Debes revisar tus opciones de privacidad, para definir quién puede ver tu cuenta y quién no.
Denuncia:
Si alguien te ha suplantado debes denunciarlo, tanto a la propia red social como a la policía, ya que se trata de un delito. Misma solución si sufres de ciberacoso.
Desconfía:
No te fíes de las peticiones de amistad de gente que no conozcas. Comparte tus contenidos únicamente con personas que conozcas en la vida real.
Corrobora:
No te creas todas las noticias que ves en las redes sociales. Antes de difundirlas, comprueba y contrasta por otros medios, digitales o no, que se trata de una noticia real.

La protección del consumidor ante la publicidad digital

Internet es una gran ventana de información y de recursos pero como consumidores tenemos que tener un espíritu crítico y responsable, especialmente si no se quiere que la información que se comparte caiga en manos de terceros. Los datos personales de los usuarios suponen un valor muy importante para las empresas y debemos aprender a proteger nuestros datos al navegar por Internet.

Eres lo que publicas

La principal acción para autoprotegernos en la red es actuar preventivamente, es decir, no dando nuestro consentimiento al tratamiento de nuestros datos en aquellos acuerdos de los que dudemos o no hayamos solicitado. En ocasiones estos acuerdos suelen venir acompañados de regalos, ofertas o descuentos.

A continuación veremos una serie de recomendaciones para autoprotegerse en Internet adoptando una posición precavida ante las posibles exposiciones con las que nos topamos en la era digital.

- **Publicidad no deseada**

Inscríbete en **https://www.listarobinson.es** para evitar publicidad de empresas a las que no hayas dado tu consentimiento para que te envíen publicidad.

- **Publicidad encubierta**

Para evitar esta publicidad encubierta se debe tener un sentido crítico de lo que te están mostrando, sin dejarse llevar por el señuelo, como que esté garantizado por personas famosas.

- **Pautas para una buena autoprotección**
  - » No publicar información personal, como: fecha de nacimiento, domicilio, ubicación actual, número de teléfono, etc.
  - » No facilitar datos bancarios por correo electrónico.
  - » Utiliza contraseñas seguras que nunca debes compartir ni publicar.
  - » Configura adecuadamente la privacidad de tu perfil.

Reclama

Si consideras que han sido vulnerados tus derechos puedes recurrir por distintas vías:

- Acudir a una Asociación de Consumidores, como ADICAE (**www.adicae.net**), para solventarlo.
- Sistema público de resolución extrajudicial de conflictos a través de las Juntas Arbitrales de Consumo de tu Comunidad Autónoma.
- Agencia Española de Protección de Datos. En su página web **www.aepd.es** podrás encontrar información acerca de cómo tramitar tu reclamación.

El buen uso de las aplicaciones móviles

Desde el mismo momento que se popularizó el uso de *smartphones*, también lo hicieron las aplicaciones móviles. Desde aplicaciones de mensajería, juegos y de consulta (ya sea noticias o el tiempo), hoy en día hay aplicaciones para cualquier necesidad que se nos pueda ocurrir.

Además muchas de esas aplicaciones son gratuitas y es tan sencillo descargarlas que, en ocasiones, olvidamos algunos puntos clave, como son el modo de pago (ya sea de la aplicación o de complementos dentro de la misma), los datos que recolecta de nuestro móvil, quién accede a esa información o que uso le darán.

Por ello, es importante seguir una serie de pautas antes de descargarse cualquier aplicación:

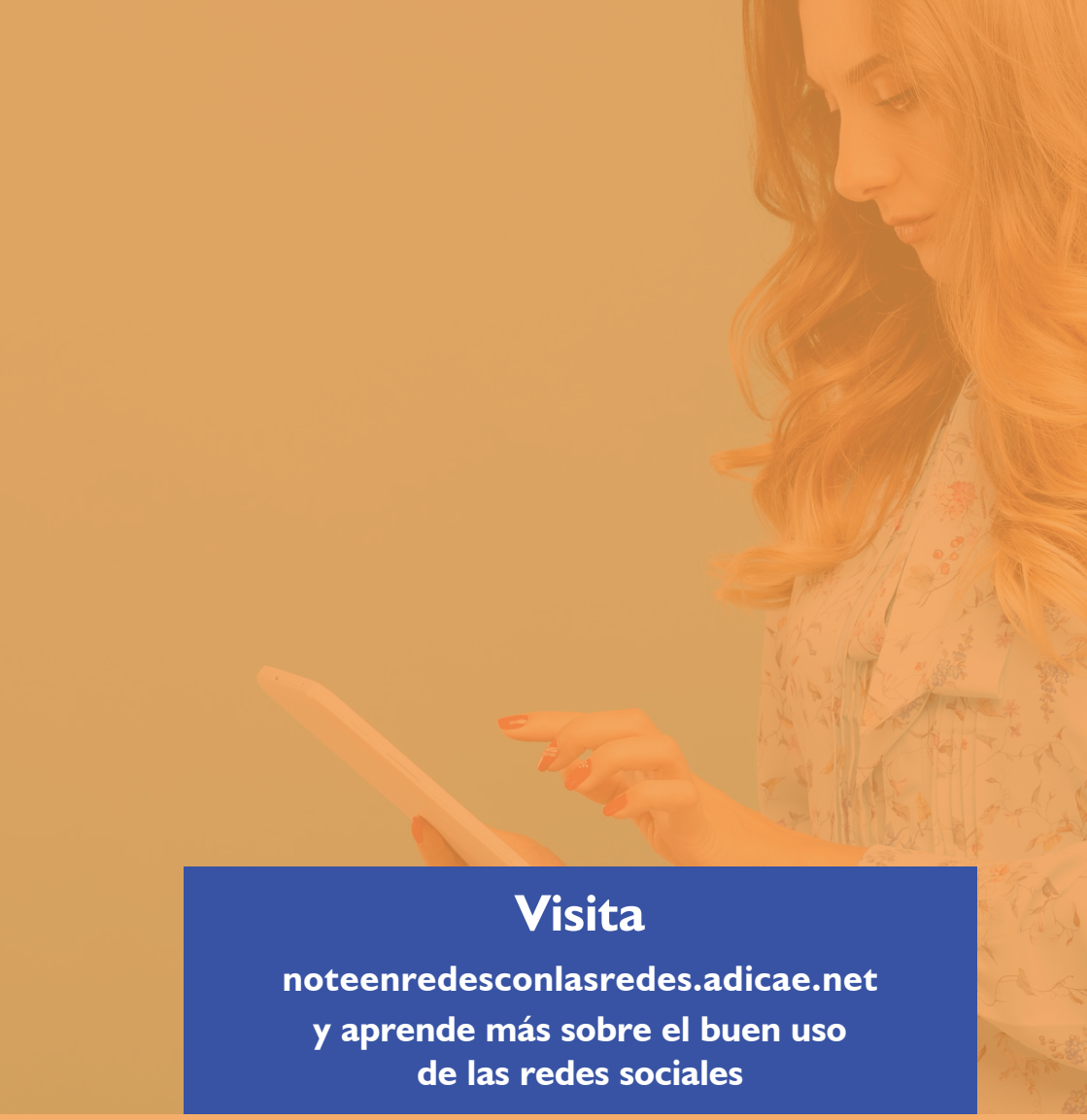
- Descarga aplicaciones únicamente desde **tiendas oficiales** (Google Play para smarphones Android y App Store para iPhones).
- Asegúrate de que la **aplicación es legítima**. Habitualmente hay copias falsas que pueden introducirte algún tipo de *malware*.
- Comprueba que quien ha desarrollado la aplicación cuenta con la validación oportuna.
- **Lea atentamente el proceso de instalación** para evitar la compra e instalación de otras aplicaciones o complementos que no deseas.

Aplicaciones recolectadoras de datos

Al descargar una aplicación, habitualmente nos pide la autorización para que demos permiso a acceder a cierta información de nuestro Smartphone. Algunos de los permisos que piden son:

- Contactos de teléfono y email
- Registro de llamadas
- Información del calendario
- Geolocalización
- El uso de la propia aplicación
- Acceso a la cámara
- Acceso a las fotografías, datos multimedia y archivos. Es la más común, ya que suelen necesitar el acceso a la memoria donde guarda archivos
- Acceso al micrófono

La mayoría de las aplicaciones móviles piden el acceso a las características necesarias para el funcionamiento de la aplicación, por ejemplo, es lógico que pida acceso a la cámara una aplicación de fotografías. Sin embargo, algunas piden acceder a datos que no están relacionados con el propósito de la aplicación. Por ejemplo, muchas aplicaciones usan los servicios de geolocalización para conocer su ubicación y mandarle ofertas cuando se acerca a una tienda o, simplemente, para vender esa información a terceros. Si no quiere que tengan esa información, rechaza la solicitud de permiso o busca otra aplicación alternativa que no pida esa autorización.



Visita

noteenredesconlasredes.adicae.net

y aprende más sobre el buen uso de las redes sociales

Acude a tu sede más cercana de ADICAE.
Obtén más materiales y herramientas de aprendizaje sobre RRSS.
Conviértete en consumidor crítico, responsable y solidario

www.adicae.net

www.adicae.net

@ADICAE

@AdicaeConsumidores

@Adicae

@adicae_consumidores

GOBIERNO DE ESPAÑA
MINISTERIO DE SANIDAD, CONSUMO Y BIENESTAR SOCIAL
SECRETARÍA GENERAL DE SANIDAD Y CONSUMO
DIRECCIÓN GENERAL DE CONSUMO

Con el apoyo del Ministerio de Sanidad, Consumo y Bienestar Social.
Su contenido es responsabilidad exclusiva de la Asociación.