

La Publicidad, las compras y el ocio en Internet.





ÍNDICE

I. OBJETIVOS.....	3
II. CONCEPTOS.....	3
1. CONCEPTOS E IDEAS CLAVE.	3
a) Email marketing.....	3
b) Rastreo de la actividad de los usuarios en la red con fines comerciales.	4
c) Cookies.....	5
d) Rastreo de móviles (Mobile tracking)	7
e) Los riesgos del rastreo online.....	7
f) Los juegos online.	8
g) Las compras en Internet.....	9
2. CONSEJOS.....	10
3. ENLACES DE INTERÉS.	11
III. ACTIVIDADES.....	13
1. EL EDUCADOR LEERÁ EL SIGUIENTE SUPUESTO.....	13
2. SMS	13
3. GEOLOCALIZACIÓN.	14



I. **OBJETIVOS**

- › Conocer las prácticas comerciales y publicitarias utilizadas en Internet y los riesgos que conllevan para la protección de los datos personales de los usuarios.
- › Tomar conciencia de los riesgos para la privacidad asociados a los videojuegos online.

II. **CONCEPTOS**

1. **CONCEPTOS E IDEAS CLAVE.**

El uso masivo de Internet ha traído consigo un extraordinario desarrollo del comercio electrónico y de nuevos modelos de negocio basados en la publicidad que se dirige a los usuarios de la Red. Baste señalar que para un importante número de sitios Web, entre ellos algunos de los más relevantes, la publicidad online constituye su mayor fuente de ingresos. Para llegar al consumidor, las empresas utilizan diferentes técnicas y estrategias que iremos viendo a lo largo de esta ficha.

a) Email marketing.

Es una forma de marketing que consiste en el envío de **correos electrónicos** que contienen mensajes comerciales. Las empresas aprovechan sus bases de datos de clientes o usuarios registrados para dirigir campañas de publicidad personalizada a éstos, a menor coste y con mayores posibilidades de comunicación que con el envío postal tradicional. En ocasiones el envío de estos mensajes comerciales puede realizarse por medio de SMS.

La ley establece garantías para protegernos como usuarios frente a un posible uso inadecuado de estas prácticas:

- › El mensaje debe reflejar claramente la identidad del anunciante.
- › El carácter publicitario del mensaje debe resultar inequívoco.
- › Antes de enviarnos publicidad, el anunciante debe pedir nuestra autorización.
- › El anunciante debe facilitarnos, de manera obligatoria, una dirección electrónica para comunicarle que no deseamos seguir recibiendo mensajes publicitarios.



b) Rastreo de la actividad de los usuarios en la red con fines comerciales.

La mayoría de usuarios de Internet hemos tenido la experiencia de visitar un sitio Web que incluye anuncios dirigidos a nuestros gustos o intereses, o que es capaz de recordar nuestras preferencias de visita en visita. Estas situaciones constituyen ejemplos de la denominada **publicidad online basada en el comportamiento** (Online Behavioural Advertising), que se caracteriza por personalizar el tipo de mensaje publicitario que se muestra al usuario al visitar una página Web basándose en su perfil, entendido éste como el conjunto de sus características, gustos, intereses y preferencias. La construcción del perfil de los usuarios se realiza a partir de la recolección de trazas de su actividad de navegación (**behavioural tracking**): sitios y páginas visitadas, contenidos accedidos, búsquedas realizadas, etc. Estos datos son procesados posteriormente aplicando técnicas de minería de datos, de forma que sea posible elaborar el perfil del usuario, incluyendo características como la edad y el género, o los hábitos de compra.

El uso de técnicas de rastreo online nos aporta beneficios como usuarios en la medida en que recibimos información útil y anuncios online relevantes que están enfocados a aquello que nos interesa. Sin embargo, también conlleva riesgos para nuestra privacidad, puesto que se apoya de forma importante en el tratamiento de datos personales. Un uso inapropiado de estas tecnologías podría llevarnos a una sociedad o Internet vigiladas, donde toda nuestra actividad online o incluso física es registrada e interrelacionada.

Los menores constituyen un colectivo prioritario para la publicidad en Internet, debido a su uso intensivo de la Red y por su mayor inclinación a seguir las modas y últimas tendencias. Este hecho, junto con una actitud en general menos crítica y más confiada hacia los mensajes que se muestran en Internet, hace que se trate de un colectivo más vulnerable frente a posibles prácticas que supongan un riesgo para la privacidad.



Es importante destacar que buena parte de las redes sociales más populares rastrean la actividad de los usuarios en la Red. Cada una de estas redes sociales dispone de widgets o botones para compartir o recomendar contenidos que están instalados en numerosos sitios Web. Estos botones permiten a las redes sociales rastrear la actividad de los usuarios, incluso aunque no hagan click en ellos: es suficiente con visitar la página Web en la que dichos botones se encuentran instalados..

c) Cookies

El rastreo de nuestra actividad en la red puede hacerse con diversas tecnologías, siendo las cookies la más extendida. **Una cookie es un fichero que se almacena en el navegador del usuario cuando éste visita una página web.** Las cookies se utilizan para registrar, almacenar y compartir información sobre nuestra actividad en la red. También pueden usarse para personalizar la forma en que navegamos en Internet, o para mostrarnos anuncios específicamente orientados a nuestros intereses.

Existen diferentes tipos de cookies. Las cookies de sesión son cookies temporales usadas frecuentemente para almacenar opciones de usuario o el estado de navegación. Se crean cuando iniciamos una sesión de navegación en un sitio web y se borran generalmente cuando cerramos el navegador. Por su parte, las cookies persistentes permanecen almacenadas en nuestro navegador hasta que las borramos de manera intencionada o expiran después de un tiempo establecido por el responsable de la cookie, que puede ir de unos minutos a varios años. Las cookies persistentes son reenviadas por nuestro navegador al sitio web cada vez que accede a él, por lo que pueden ser utilizadas para hacer un seguimiento de nuestras visitas a esa página web. Este hecho hace que el uso de cookies persistentes plantee riesgos para la privacidad de las personas. Las cookies también se pueden clasificar según la entidad que las controla y desde cuyos servidores web se envían al navegador del usuario. Las cookies propias son aquellas que se envían al equipo del usuario desde el propio sitio web que está visitando. En general, su finalidad es hacer más eficiente nuestra navegación en esa página web. Por ejemplo, pueden ayudar a los sitios web a recordar los productos que vamos añadiendo a la cesta de compra de un portal de comercio electrónico, nuestro nombre de usuario, nuestras preferencias (como mostrarnos la previsión del tiempo



Ficha didáctica
**La Publicidad, las Compras
y el Ocio en Internet.**

05



en nuestra localidad), o las puntuaciones anteriores obtenidas en un videojuego online.

Las cookies de terceros son almacenadas en nuestro navegador por otras entidades distintas de la que controla el sitio web visitado. Pueden ser utilizadas para mostrarnos mensajes publicitarios dirigidos específicamente a nuestros intereses o preferencias. Por ejemplo, si leyéramos un artículo sobre jardinería en un periódico digital, podría utilizarse una cookie de terceros para registrar este hecho y añadirlo a nuestro perfil de usuario, de forma que en sucesivas visitas se nos mostraran mensajes publicitarios relacionados con productos de jardinería. Muchas compañías publicitarias usan este tipo de cookies para rastrear la actividad de los usuarios a lo largo de múltiples sitios Web. El conocimiento de las páginas visitadas por el usuario les permite mostrarle mensajes publicitarios dirigidos de manera específica a lo que se presume son sus intereses o preferencias.

La mayoría de navegadores permiten controlar qué cookies pueden almacenarse en el equipo del usuario. El bloqueo total de las cookies puede hacer más incómoda nuestra navegación en la red, obligándonos por ejemplo a introducir datos de forma reiterativa. No obstante, la mayor parte de los navegadores permiten bloquear las cookies de terceros sin afectar a las cookies propias de los sitios web visitados.

La Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (LSSI), requiere que los sitios web (prestadores de servicios) que utilicen cookies informen a los usuarios de manera completa sobre la finalidad para la que se instalaron y los usos que se les darán y obtengan su consentimiento para la recolección de datos. Obligación que alcanza a todas las cookies excepto a aquellas cuya finalidad es la de permitir únicamente la comunicación entre el equipo del usuario y la red, o son estrictamente necesarias para prestar un servicio expresamente requerido por el usuario.



d) Rastreo de móviles (Mobile tracking)

Las tecnologías de rastreo de la actividad online de los usuarios se han extendido de manera significativa con el uso creciente de *smartphones* (teléfonos inteligentes), que ha traído consigo el desarrollo de numerosas aplicaciones (comúnmente conocidas como Apps) que registran la localización y movimientos de los usuarios. La **geolocalización** permite ofrecernos servicios útiles, como consejos sobre qué dirección tomar cuando estamos en un atasco, conocer dónde están nuestros amigos, o recibir recomendaciones sobre restaurantes situados en la zona en la que estamos. Sin embargo, esta información se utiliza en ocasiones también con la finalidad de elaborar perfiles de los usuarios.

Un reciente estudio publicado en la prensa revelaba que algunas de las aplicaciones para iPhone o Android más populares transmitían la localización del móvil, edad, género y otros datos personales a terceras empresas sin el conocimiento o consentimiento de los usuarios.

Algunas redes sociales nos animan a compartir nuestros datos de localización y la información que publicamos en otras puede ser usada para deducir si nos encontramos en nuestro domicilio o no. Otras aplicaciones nos permiten conocer la localización de los móviles de nuestros amigos en tiempo real y mostrarla sobre un mapa.

e) Los riesgos del rastreo online.

Si bien el uso de tecnologías de rastreo en la Red conlleva beneficios indudables para la actividad económica y para los usuarios, también plantea riesgos para la privacidad. Entre ellos se pueden destacar los siguientes:

- › **Vigilancia y control global** de nuestra actividad en la red, que podría ser llevado a cabo por los Estados, por razones políticas o de seguridad nacional, o por empresas por razones comerciales. Existen modelos de predicción que, analizando cambios en las pautas de navegación de los usuarios, pueden deducir, por ejemplo, si una mujer está embarazada o si una persona se está divorciando.



- › **Discriminación de servicios y de precios.** La elaboración de perfiles puede revelar que un usuario padece una determinada enfermedad, o tiene cierta propensión a desarrollarla. Esta información podría ser usada, por ejemplo, por una aseguradora médica para denegarle la contratación de una póliza de salud, o para aplicarle una penalización adicional en la cuota que debe abonar por este servicio.
- › **Excesiva personalización** de la información que se muestra al usuario, que podría quedar atrapado en una “burbuja de filtros y contenidos” y no estar expuesto a información que podría ampliar su visión de las cosas. En estados con regímenes autoritarios, esta personalización podría ser utilizada con fines de censura, seleccionando de forma controlada las noticias mostradas a determinados usuarios.

f) Los juegos online.

En los últimos años se han popularizado los videojuegos online, en los que, mediante el ordenador, la videoconsola o un *smartphone*, podemos jugar con otros usuarios que están conectados a Internet. Esta forma de jugar nos abre nuevas posibilidades para disfrutar más nuestro tiempo de ocio, pero también conlleva algunos riesgos para nuestra privacidad de los que debemos ser conscientes.

Para participar en juegos online, la página Web nos va a solicitar que nos identifiquemos como usuarios del juego, lo que hace posible que pueda asociar a ese perfil de usuario toda nuestra actividad en él. El riesgo es que no conocemos en realidad con quién estamos jugando o con qué finalidad se va a utilizar la información que el sistema ha registrado sobre nosotros. Por este motivo, debemos ser muy prudentes cuando nos soliciten información para abrir una cuenta y participar en el juego, evitando proporcionar datos personales que nos puedan identificar.

En muchos casos, el videojuego incorpora funcionalidades como chat con texto, voz o imagen, o una red social asociada para compartir información, por lo que los riesgos para la privacidad pueden ser los mismos que los presentes en este tipo de aplicaciones de Internet. De hecho, se han dado casos en los que un usuario malintencionado, usando una identidad



Ficha didáctica
**La Publicidad, las Compras
y el Ocio en Internet.**

05



falsa, aprovechaba las posibilidades de juego colaborativo online de una conocida videoconsola dotada de videocámara, para ganarse la confianza de menores, a los que invitaba a visitar páginas con contenido sexual para adultos y conseguir imágenes comprometedoras de estos jóvenes, con la finalidad de extorsionarles posteriormente.

También debemos estar alerta contra algunas prácticas que, aunque no podemos considerar generalizadas, debemos conocer, como la existencia de videojuegos online que incitan a realizar apuestas o desembolsos económicos (por ejemplo, para hacer nuestro personaje más potente), o que susciben a los usuarios a servicios SMS Premium de alto coste.

g) Las compras en Internet

Debido a su condición de usuarios intensivos de la Red, los menores constituyen un objeto prioritario para muchas compañías que venden sus productos en Internet. Por ejemplo, cada vez son más los servicios que aparecen y que permiten descargarse música, juegos, aplicaciones, etc. en el teléfono móvil.

La compra de productos en Internet nos permite acceder a una oferta muy amplia de productos sin movernos de casa, pero debe hacerse adoptando precauciones que nos eviten sorpresas desagradables. Por ejemplo, algunas empresas pueden realizar promociones fraudulentas con la finalidad de contratar servicios *SMS Premium* que nos podrían ocasionar un grave perjuicio económico.

Por esta razón, es aconsejable que cualquier compra que quiera hacer un menor por Internet esté supervisada por un adulto responsable, que pueda orientarle y comprobar si el sitio Web es de confianza. Un caso muy habitual de compra online es la descarga de aplicaciones en nuestro *smartphone*. Es importante comprobar si la descarga tiene un coste asociado, y preguntar antes a los padres para evitar disgustos en la factura.

Antes de realizar cualquier compra en la Red debemos comprobar si el sitio web es de confianza, por ejemplo verificando que dispone de política de privacidad, y que emplea tecnologías que permiten un intercambio seguro de datos. La presencia del término "*https*", o de un candado en la dirección web visitada que muestra el navegador cuando vamos a transmitir datos como nuestra contraseña o nuestro número de tarjeta de crédito, es una señal de que el sitio web



se está comunicando de forma segura con nuestro equipo. Debemos tener presente que el correo electrónico no es un medio seguro para realizar compras en la Red, por lo que no debemos confiar en mensajes que nos solicitan datos financieros por este medio.

2. CONSEJOS

- › Las ventanas emergentes, o *"pop-up"*, que se abren cuando se visitan algunas páginas Web pueden contener anuncios o presentar ofertas especiales tras las cuales se puede ocultar la instalación de un software malicioso, por lo que debemos proteger nuestro equipo con un software anti virus debidamente actualizado.
- › Con objeto de evitar que se pueda realizar un seguimiento de las visitas efectuadas a otros sitios web, es recomendable borrar del equipo periódicamente los archivos temporales y las *"cookies"*, teniendo en cuenta que, en este último caso, el usuario puede configurar el navegador para evitar la grabación de las *"cookies"* en el equipo.
- › El correo electrónico no es un medio seguro para realizar compras en la Red, por lo que no debemos confiar en mensajes que nos solicitan datos financieros por este medio.
- › Las compras realizadas por un menor en Internet deben estar supervisadas por un adulto que pueda verificar que el sitio web es de confianza y las condiciones comerciales. Por ejemplo, en el caso de descargas de aplicaciones en el móvil debemos comprobar previamente si es gratuita o tiene un coste.
- › Al acceder a un portal de comercio electrónico, es aconsejable hacer un pequeño esfuerzo en conocer los servicios y el tipo de información a que se puede tener acceso. La existencia de políticas de privacidad comprensibles, la identificación del responsable del servicio con todos los datos necesarios para localizarle, la presencia de información sobre el modo de contratar, o la utilización de conexiones seguras para facilitar los datos o gestionar los pagos, son datos que deben ser tenidos en cuenta antes de utilizar este tipo de servicios.



- › Al realizar compras en Internet, verificar que se ha establecido una conexión segura entre nuestro dispositivo y el servidor de Internet antes de facilitar ningún dato personal, incluidos códigos de usuario y contraseñas. La existencia de una conexión segura puede identificarse mediante la aparición del acrónimo “https” o de un candado en la barra de direcciones del navegador.
- › Es aconsejable realizar las compras en Internet mediante una tarjeta de crédito específica para estos fines, con límite de gasto reducido.
- › Es preferible descargar nuestros juegos y aplicaciones desde sitios oficiales de fabricantes y desarrolladores.
- › Desactivar las restricciones impuestas por el fabricante de un videojuego, consola u otro dispositivo puede eliminar sus medidas de protección.
- › Cuando participemos en un videojuego online no debemos facilitar datos personales que nos puedan identificar, por lo cual es aconsejable usar un alias o nick anónimo como nombre de usuario. Asimismo, debemos desconfiar de aquellos jugadores que nos hagan preguntas sobre nuestra vida personal o pretendan obtener imágenes nuestras.

3. ENLACES DE INTERÉS.

- › AEPD - Guía sobre el uso de las Cookies
http://www.agpd.es/portalwebAGPD/canal/documentacion/publicaciones/common/Guias/Guia_Cookies.pdf
- › GT29 - Dictamen sobre la extensión del requisito de consentimiento de cookies:
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp194_es.pdf
- › GT29 - Dictamen sobre publicidad comportamental en línea:
http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_es.pdf



Ficha didáctica
**La Publicidad, las Compras
y el Ocio en Internet.**

05



- › GT29 - Dictamen sobre la recomendación de mejores prácticas de EASA/IAB sobre publicidad comportamental en línea:

http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp188_es.pdf

- › ENISA - Consideraciones sobre privacidad y publicidad comportamental:

<http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/privacy-considerations-of-online-behavioural-tracking>

- › INTECO - Guía de seguridad y privacidad en el comercio electrónico:

http://www.inteco.es/Seguridad/Observatorio/guias/Guia_seguridad_privacidad_comercio_electronico

- › INTECO - Guía para padres y madres sobre el uso seguro de videojuegos:

http://www.inteco.es/Seguridad/Observatorio/guias/guia_menores_videojuegos



III. ACTIVIDADES

1. EL EDUCADOR LEERÁ EL SIGUIENTE SUPUESTO.

“El otro día María le estaba contando a Luis lo que le había ocurrido a su hermana. Resulta que recibió una llamada de alguien que dijo llamarla de una compañía de telefonía móvil ofreciéndole una promoción. Le ofrecían una tarjeta que le permitía hacer llamadas gratis todos los fines de semana y entre semana muy baratas. Pero para poder tener la promoción tenía que dar todos sus datos por teléfono, incluido el número de la tarjeta de crédito y le enviarían la tarjeta a casa. Además, podía dar el contacto de un amigo y así recibiría una tarjeta más. Cuando quiso darse cuenta su hermana tenía 100 euros menos en su tarjeta de crédito”.

1. ¿Cómo podemos protegernos ante este tipo de estafas?

2. SMS

El educador leerá el siguiente mensaje que podría haber llegado a cualquier teléfono móvil:

“¡Enhorabuena! Has sido seleccionado para ganar 3000 euros. Sólo tienes que mandar la palabra GANAR al 25634 y entrarás en el sorteo. Coste del mensaje 1,42 euros”

1. ¿Qué os parece el mensaje?
2. ¿Os fiaríais de él?



3. ¿Sabéis dónde podéis denunciar este tipo de mensajes?

Podéis tramitar una denuncia en la Agencia Española de Protección de Datos.

Han sido muchas las denuncias que se están realizando ante la Agencia Española de Protección de Datos. Este tipo de mensajes suelen tener como resultado una suscripción a un boletín por la que te van cobrando por mensaje recibido. En muchos casos el usuario desconoce el mecanismo para cursar la baja del servicio.

3. GEOLOCALIZACIÓN.

El otro día a Carla, la llamaron unos amigos para ir al cine. La verdad es que el día anterior había propuesto a otro grupo de amigos irse de fin de semana a la casa del pueblo de uno de ellos. Carla puso la excusa de que se quedaba en casa porque estaba con gripe. Realmente se fue de viaje. No cayó en la cuenta de que en su Smartphone, y en el de todos sus amigos, tenían instalada una aplicación de "geolocalización" para saber dónde estaban cada uno de ellos en todo momento y que se le había olvidado desactivarla, por lo que todos sus amigos supieron dónde había pasado el fin de semana...

1. ¿Qué crees que habrán sentido sus amigos al enterarse de que realmente no estaba en casa con gripe?
2. ¿Te parece seguro que todo el mundo pueda saber dónde estás en cada momento?
3. ¿Cómo podría haber evitado las consecuencias?