BOLETÍN INFORMATIVO DEL CONSUMIDOR
Publicación Mensual. Nº 1.- Febrero 2004

O M I C

EXCMO. AYUNTAMIENTO DE ANDUJAR.
DELEGACIÓN MUNICIPAL DE CONSUMO

TITULARES:

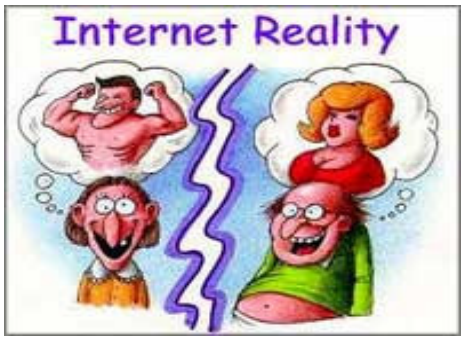
- Consejos Generales.
- Navegación.
- Correo electrónico.
- Compras en Internet.
- La publicidad no deseada.
- Los timos de las conexiones a los 800

Consejos básicos de seguridad para los usuarios de Internet

Consejos Generales

Utiliza el sentido común

En algunas ocasiones hacemos en Internet algo que nunca haríamos en una situación similar en la vida real. El hecho de que sea un medio nuevo no debe hacernos perder la



cordura.

Utiliza siempre la última versión de los programas

Continuamente aparecen nuevos agujeros de seguridad en los navegadores y en los programas que habitualmente se utilizan en Internet (correo electrónico, chat, etc.). Utiliza la última versión disponible, que se supone será más segura que las anteriores

Virus

En la actualidad más del 75% de los virus se propagan a través de Internet en sus diferentes aplicaciones. Recuerda que un Virus te puede hacer perder toda la información de tu ordenador e incluso de tu red y además puedes pasárselo a tus conocidos (a aquellos con los que intercambias información) a través de la red y sin que te des cuenta.

Navegación

Cierra las puertas del ordenador que utilizas para navegar por la red

Si utiliza un ordenador con Win 9x, los intrusos o hackers pueden conseguir acceso cuando está configurado para compartir

archivos e impresoras. Incluso si no se encuentra en una red, la configuración de su PC puede permitir compartir ficheros... ¡y la entrada de hackers!

Para deshabilitar compartir ficheros e impresoras en Windows 9x, seleccione Inicio-->Configuración-->Panel de control, haga doble clic en el icono de Red y seleccione la pestaña de Configuración. Presione el botón Compartir archivos e impresoras y asegúrese de que ambas casillas en el cuadro de diálogo están sin habilitar, "Permitir que otros usuarios tengan acceso a mis archivos" y "Permitir que otros usuarios impriman en mis impresoras".

No reveles datos personales si no es necesario

A menudo al navegar por la Red nos encontramos con formularios que nos piden ciertos datos personales. Rellena sólo aquellos que consideres sean relevantes para el servicio que se ofrece y no

des el resto, si son obligatorios para poder avanzar en la petición utiliza datos ficticios.

Entérate de las políticas respecto a la privacidad

Exige en los web que te piden datos e incluso en aquellos que utilizas habitualmente que te informen sobre que datos recogen de tu navegación y para que la utilizan, si no encuentras esta información desconfía de ellos.

Correo Electrónico

Cifra y firma los correos

Si no quieres que cualquiera lea tus correos, pero te interesa conservar tu identidad, cifra los correos y fírmalos. Así el destinatario estará seguro de que nadie más lee los mensajes que tú y sólo tú le envías. Si sólo aceptas como válidos los correos firmados no te expones a

que nadie suplante la personalidad (spoofing) de otro y te engañe.

Usa distintas cuentas de correo

Utiliza cuentas de correo especificas para suscribirte a grupos de noticias, para ponerlas en páginas web, etc. De esta forma evitaras que tu correo de trabajo se vea inundado de correos comerciales no deseados y cuando quieras podrás dar de baja esa cuenta sin afectar a otras actividades.

Utiliza la copia oculta para enviar correos

Cuando envíes copias de un correo a más gente pon la lista de direcciones a enviar en el apartado de BCC o CCO (Blank Copy o Copia Carbón Oculta) en lugar de utilizar el campo CC (Carbon Copy) salvo que tengas interés en que se sepa a quien le has enviado copia de tu correo. De esa forma evitarás que los destinatarios tengan tu lista de correo y puedan hacer un uso indebido de la misma.

Correos no solicitados; Spam

No te quedes impasible ante la

recepción de correos no solicitados ya que este problema nos afecta a todos y nos hace perder mucho tiempo , dinero y recursos.

Compras en Internet

Utiliza solo servidores seguros para comprar (aquellos que empiezan por https://..) , nunca deberías suministrar información confidencial por Internet sin ningún tipo de protección, especialmente en lo que se refiere a datos financieros, *(números de cuentas o libretas de ahorro, números de tarjetas de crédito)*.

No entregues más información que la estrictamente necesaria para recibir el producto que has comprado.

No envíes tu número de tarjeta de crédito por correo electrónico.

Comprueba rutinariamente los certificados de los sitios seguros a los que te conectas

Reclama tus derechos como consumidor, exige información detallada y clara sobre los precios, sobre la forma de envío y coste adicional y las condiciones de garantía y devolución.

Busca la página sobre política de privacidad del comercio, para saber qué se hace con tu información privada, tanto la recopilada directamente, suministrada al rellenar formularios, como la obtenida indirectamente por tu navegación. Si no la encuentras, exígela.

No pagues en efectivo, ni con cheque, ni con tarjeta de débito, mejor hazlo con tarjeta de crédito. Es más seguro de lo que generalmente se cree y te ocasionará menos problemas en caso de irregularidades con la entrega de tu compra o fraude con tu tarjeta. Consulta con tu banco las condiciones de resolución de disputas con el comerciante. En general la entidad financiera de medios de pago te devolverá el dinero de la transacción, si has pagado con tarjeta de crédito y haces la reclamación durante los tres meses que siguen a la compra.

AGENCIA DE PROTECCIÓN DATOS

Publicidad no deseada

Preguntas frecuentes sobre Marketing Viral

Qué es un programa de marketing viral

La Asociación de Usuarios de Internet está recibiendo quejas y consultas de usuarios que ven aparecer de forma espontánea en

su ordenador mensajes y ventanas publicitarias que ellos no han solicitado. Aparecen de vez en cuando, al navegar en determinadas páginas o incluso al teclear en nuestro navegador determinadas palabras clave. Los responsables de este fenómeno

son **programas de marketing viral** que se han instalado en el ordenador del usuario generalmente sin su conocimiento.

Estos programas se comportan igual que un virus troyano. Entran desde algunos programas gratuitos que se encuentran en la Red, por e-mail, desde páginas web que instalan algún componente (normalmente desde páginas de contenidos para adultos, chat, casinos on-line, ..) o, simplemente, visionando una página de un anunciante que usa esta aplicación comercial.
Al instalarse se altera nuestro sistema operativo y a partir de ese momento el usuario cree que navega con su explorador pero realmente lo hace a través de este programa publicitario.

La agresividad de este "marketing vírico" permite, por ejemplo, visualizar publicidad de nuestra empresa cuando se visitan los webs de nuestros competidores e incluso, en algún momento, esta publicidad sustituye a los anuncios de la página original por los del competidor.

Estas intrusiones ilegítimas en la privacidad de los usuarios ya ha tenido sus primeras repercusiones a nivel judicial. Editores de los principales medios de comunicación en EE.UU. han demandado recientemente a Gator, una de las primeras empresas dedicadas a desarrollar este "marketing viral", por estas prácticas poco éticas. Pero la empresa, lejos de abandonar este camino, ha inaugurado nuevos métodos como el "one-click opt-install", es decir, las descargas de su programa al pinchar en un anuncio, con mensajes confusos para los usuarios.

Los anunciantes, por su parte, cuentan con fórmulas para intentar esquivar su responsabilidad como por ejemplo poner en marcha campañas de publicidad con técnicas piramidales que convierten a cada usuario de estos programas en un vendedor on-line a través de su web y su correo y también off-line a través del boca a boca.

¿Quién me ha instalado este programa de publicidad vírica?

Esta es la pregunta más difícil de contestar, estos programas se pueden introducir en nuestro ordenador por alguno de estos métodos:

➪ Al instalar otros programas que se anuncian como gratuitos ya que muchos ellos están recurriendo a esta publicidad como fuente de ingresos. En algunos casos se avisa en las condiciones de uso aunque casi siempre en Inglés, en letra pequeña y con términos equívocos (Permission Marketing, Matriz Viral Marketing, ...).

➪ Desde páginas web que instalan algún componente Active-X que se utiliza para otro fin (programas para chats, visores especiales de video y audio, etc. Son muy populares en los webs de contenido pornográfico y en los webs dedicados a apuestas y casinos on-line.

➪ Desde las páginas web de los propios fabricantes o

anunciantes que utilizan este sistema.

➪ A través de ficheros ejecutables y de comandos que nos llegan a través del correo electrónico.

¿Qué programas recogen datos personales?

Programas que encontrar en su ordenador que espían su actividad y que recaban información sobre los usuarios para enviarla a las casas publicitarias son entre otros estos: Webhancer, Customer Companion, Conducent/Timesink, Cydoor, Comet Cursor, Web3000, Audiogalaxy, Babylon Tool, Copernic 2000, CrushPop, CuteMX, EZForms, Gator, FlashGet, Gif Animator, iMesh, JPEG Optimizer, MP3 Downloader, MP3 Fiend, NeoPlanet Browser, Net Scan 2000, Net Tools 2001, NetMonitor, Odigo Messenger, Opera Freeware, Oligo Browser, Real Audioplayer, Spam Buster, TIFNY, TypeItIn, WebCopier, ZipZilla.

¿Cómo evitar que me pase a mi?

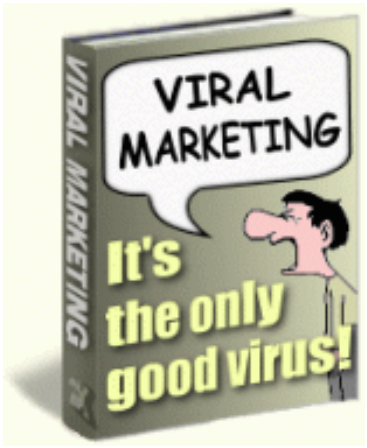
Los consejos para evitar el que te cuelen este tipo de programas en tu ordenador son los mismos que te protegen contra los virus

informáticos. Utilizar ultimas versiones de los navegadores, configurar la seguridad y la privacidad a nivel alto, no ejecutar ni instalar ningún programa si no se quién es la fuente del mismo (no confundir la fuente con el que me lo envía o me lo pasa), proteger los ficheros del sistema, disponer siempre de copias de seguridad, ...

¿Son peligrosos los programas gratuitos que encuentro en Internet

Estas son algunas reflexiones que hace Gonzalo Álvarez Marañón especialista en seguridad del Instituto para la Seguridad en Internet al respecto:

Los programas gratuitos son muy frecuentes en Internet. ¿Nunca se ha preguntado por qué contra toda lógica una empresa puede decidir ofrecer software gratis? ¿Qué obtiene a cambio? La respuesta casi siempre es la misma: sus datos personales. La próxima vez que descargue un programa sin que le cobren por ello, piense que a lo mejor no es tan gratuito como se anuncia en la publicidad. Sus datos personales pueden suponer el precio que pagará por él.



El pagar con su privacidad a cambio de obtener un programa en apariencia gratuito se está convirtiendo en moneda de cambio común en Internet. Con eso de que cada vez más usuarios tienen su ordenador conectado a la Red, incluso de forma permanente gracias a tarifas planas de cable y ADSL, muchas compañías optan por distribuir sus productos de forma totalmente gratuita y cobrarse el servicio espiando la actividad del usuario.

Siempre que instala un programa en su ordenador, éste necesariamente tiene acceso a todos los recursos del sistema: puede leer cualquier rincón del disco duro, registrar cada pulsación de teclado realizada por el usuario o guardar un histórico de cada programa y documento abiertos. Claro que una cosa es la posibilidad de llevar a cabo todas estas tareas y otra, que se haga de verdad.

Los programas que rastrean la información sobre hábitos de consumo y navegación de los usuarios de Internet pueden realizar todas o alguna de las actividades anteriores de manera sigilosa, sin que nadie lo advierta. A intervalos de tiempo programables, el programa se conecta a través de Internet con un servidor de la compañía que lo distribuyó y transmite diligentemente toda la información que ha recopilado.

Por otro lado, las barras de navegación constituyen la última vuelta de tuerca en las novedosas estrategias maquinadas por las empresas punto com, para recabar subrepticiamente información sobre los usuarios. Existen docenas de barras gratuitas que asisten al usuario de Internet en su navegación: le facilitan las búsquedas en Internet, le proporcionan información extendida sobre el sitio que está visitando, le ayudan a comparar precios sobre productos, en definitiva, colaboran para que su vida en la Red sea más sencilla.

Lo que el usuario de Internet desconoce es que, silenciosamente entre bastidores, algunas barras también registran cada página que visita, cada formulario que rellena, sin distinguir si se trata de páginas cifradas o no. Cada cierto tiempo, las barras envían toda esta información a la empresa de software, que ve así recompensados con creces sus esfuerzos por desarrollar el producto "gratis". Otra forma de recopilación solapada de datos de los usuarios de Internet que se ha visto en Internet consiste en la utilización de los "Web bugs" o "escuchas Web", de las que ya se habló en un artículo anterior.

Mientras algunas compañías avisan acerca de su intención de recopilar información sobre hábitos de navegación del usuario en la letra pequeña de sus licencias de uso, ese texto que nadie lee cuando instala los programas, otras obvian toda referencia clara a su actividad espía. Obtener datos privados sobre los usuarios sin pedir su consentimiento y, lo que es peor, sin ni siquiera informarles sobre ello, representa un grave atentado contra la privacidad que se está volviendo cada vez más frecuente en Internet.

La próxima vez que descargue un programa sin que le cobren por ello, piense que a lo mejor no es tan gratuito como se anuncia en la publicidad. Sus datos personales pueden suponer el precio que pagará por él.

¿Es ilegal esta publicidad vírica?

Si se ha introducido algo en nuestro ordenador sin nuestro consentimiento se contraviene nuestro Código penal y por tanto hay una ilegalidad clara. Tal como

recoge el Capitulo IX del Titulo XIII de nuestro código penal. Se ataca el derecho a la intimida, a la privacidad, a la propiedad privada.

También se vulneran las normas básicas de publicidad, ya que el anuncio se presenta sobre un web que es ajeno al proceso (aunque todo suceda en el ordenador del usuario), probablemente estemos ante derivadas penales en aspectos como la propiedad intelectual y los derechos de marca.

Si la información que se da no es clara y precisa también se esta incurriendo en delitos y faltas que contravienen las ley de comercio que obligan a informar de forma clara y explicita.

Incluso si Vd. sabía lo que instalaba, para qué y lo autorizo también podemos estar contraviniendo la Ley de Protección de Datos de Carácter Personal (LORTAD) si no se han registrado los ficheros en la Agencia ya que se esta actuando, guardando y utilizando nuestros perfiles de uso de Internet para personalizar la publicidad.

También se han montado estructuras piramidales que ofrecen mucho dinero por una pequeña inversión prometen suculentos ingresos convirtiendo de esta forma a los usuarios de estos programas en vendedores on-line a través de sus webs y of-line a través del boca a boca.

Finalmente esta el tema ético y funcional, imaginemos que al ir a comprar el periódico a nuestro quiosco el quiosquero ha pegado unos anuncios diferentes encima de los que venían impresos, suena cuando menos un poco extraño aún y cuando tenga mi consentimiento.

Los creadores de estos programas se defienden diciendo que siempre se instalan con el permiso del usuario algo que no sucede en la realidad ya que muchos usuarios desconocen de la existencia de los mismos en sus ordenadores. Otro argumento es que la legalidad actual no entiende que hay otras formas de gestionar la publicidad y que el modelo clásico de un anuncio en un soporte esta ya caduco.

¿Qué hacer para denuncia este tipo de publicidad vírica?

Si conoce quien le instalo el programa póngase en contacto con los Cuerpos de seguridad o con la Agencia de protección de Datos para dar conocimiento de este hecho.

Cuente su caso a Asociaciones de Usuarios, de Consumidores y de Anunciantes para que a través de la información se eviten nuevos casos igual que el suyo.

CÓDIGO PENAL. TITULO XIII. CAPITULO IX

Artículo 263.

El que causare daños en propiedad ajena no comprendidos en otros Títulos de este Código, será castigado con la pena de multa de seis a veinticuatro meses, atendidas la condición económica de la víctima y la cuantía del daño, si éste excediera de cincuenta mil pesetas.

Artículo 264.

1. Será castigado con la pena de prisión de uno a tres años y multa de doce a veinticuatro meses el que causare daños expresados en el artículo anterior, si concurriere alguno de los supuestos siguientes:

1.º Que se realicen para impedir el libre ejercicio de la autoridad o en venganza de sus determinaciones, bien se cometiere el delito contra funcionarios públicos, bien contra particulares que, como testigos o de cualquier otra manera, hayan contribuido o puedan contribuir a la ejecución o aplicación

de las Leyes o disposiciones generales.

2.º Que se cause por cualquier medio infección o contagio de ganado.

3.º Que se empleen sustancias venenosas o corrosivas.

4.º Que afecten a bienes de dominio o uso público o comunal.

5.º Que arruinen al perjudicado o se le coloque en grave situación económica.

2. La misma pena se impondrá al que por cualquier medio destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos.

Artículo 265.

El que destruyere, dañare de modo grave, o inutilizare para el servicio, aun de forma temporal, obras, establecimientos o instalaciones militares, buques de guerra, aeronaves militares, medios de transporte o transmisión militar, material de guerra, aprovisionamiento u otros medios o recursos afectados al servicio de las Fuerzas Armadas o de las Fuerzas y Cuerpos de Seguridad, será castigado con la pena de prisión de dos a cuatro años si el daño causado excediere de cincuenta mil pesetas.

LOS TIMOS DE LAS LÍNEAS 800 (ANTES 906)

Los ocho fraudes y abusos más frecuentes a través de las líneas 803, 806 Y 807

Falsas ofertas de trabajo, videntes, páginas web gratuitas que suponen un gasto desproporcionado por la conexión a Internet, regalos que acaban costando menos que la llamada que hay que realizar para confirmarlos... Son algunos de los ocho tipos de fraudes y abusos más frecuentes a través de las líneas 800.

Estos son los ocho tipos de fraudes y abusos que se producen a través de las líneas 803, 806 y 807, que en octubre de 2003 han sustituido a los 906.

Ofertas de trabajo

Se anuncian generalmente en las páginas de ofertas de empleo de los diarios. Los teleoperadores realizan un largo cuestionario, prolongando

al máximo la duración de la llamada. En ocasiones, solicitan incluso una fotografía o un currículo por escrito para dar una apariencia de credibilidad al timo. Pero en realidad, nunca se recibe respuesta ya que los trabajos no existen.

Regalos y premios

El usuario recibe una llamada, una carta o un e-mail donde se le informa que ganado un sorteo o que una empresa ha decidido hacerle un regalo.

Para más información, una línea 800. La llamada a este número puede tener varios resultados: una convocatoria a una presentación comercial donde se intentará que el usuario compre un producto, cuya asistencia es indispensable para recibir el regalo; la explicación de que el regalo consiste en varias noches en un hotel o apartamento, pero con la condición de abonar la comida o unos supuestos gastos de gestión; la confirmación de un fantástico regalo, del que únicamente habrá que pagar unos gastos de envío sospechosamente altos; e incluso un largo mensaje grabado que avisa de que todas las líneas están ocupadas.

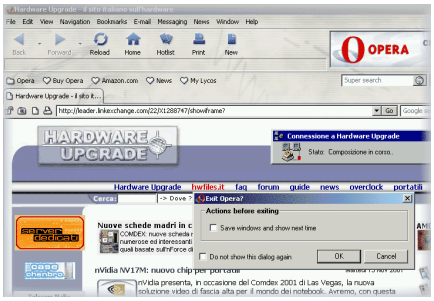
'Videntes'

Los que piensen que las artes adivinatorias son un don propiedad de privilegiados están muy equivocados. Hoy en día, cualquiera puede tener estos poderes. Y es que los supuestos adivinos, astrólogos, brujos o futurólogos

bendecidos por los medios de comunicación se han visto tan desbordados de llamadas que no han tenido otro remedio que contratar a equipos de adivinos para atender las consultas telefónicas. ¿Qué cualidades hay que reunir para ser vidente? Capacidad para retener una llamada, inventiva y un poco de psicología barata.

Páginas web 'gratuitas'

Numerosas páginas web, generalmente eróticas o



pornográficas, que se anuncian como gratuitas condicionan su visionado a que el usuario instale en su ordenador un programa, ocultando o disimulando que la función del mismo es desconectar el mode para volverlo a conectar a Internet, pero a través de una línea 80x.

Confirmaciones de pedidos

El usuario recibe un e-mail de una empresa que le anuncia que en breve le cargará en su tarjeta de crédito una cantidad en concepto de una supuesta compra que en realidad no ha realizado.

La empresa facilita únicamente un teléfono 80x para solucionar las posibles dudas que tenga el cliente. Generalmente, el usuario se intenta poner en contacto con la

empresa para anular el falso pedido a través de este teléfono, y en él un contestador retiene su llamada durante un largo rato, advirtiendo por ejemplo que las líneas están saturadas.

Concursos

En muchos casos, los cada vez más frecuentes concursos de la televisión no informan del precio de la llamada o se hace en letra pequeña. La llamada también puede prolongarse debido a mensajes excesivamente largos que el usuario tiene que escuchar antes de dejar su mensaje. En muchos casos, no se informa del tiempo que estará vigente el concurso, por lo que el usuario desconoce las probabilidades que tiene de ganar un premio que, generalmente, es de una cuantía ridícula en comparación con el coste de la llamada y el número de usuarios que participan.

Líneas eróticas

En ocasiones, lo que se presenta como una conversación erótica se reduce a una simple grabación. Asimismo, quienes atienden estos teléfonos hacen lo posible, como en

el resto de líneas 80x, por prolongar al máximo las llamadas.

Consultorios

Psicólogos, sexólogos... Cada vez más profesionales ofrecen sus servicios a través de líneas 80x. El problema es que, si bien la atención a través del teléfono deja mucho

que desear en comparación de una cita en persona, el usuario no tiene generalmente forma de comprobar si la persona que está tras la línea tiene realmente la cualificación profesional que anuncia o ésta es la misma que la de los equipos de videntes que atienden otras líneas 80x.

En cuanto a los contenidos, cada número deberá destinarse a unos contenidos determinados de la forma siguiente:

Números	Servicios
803 ABM CDU	Servicios exclusivos para adultos
806 ABM CDU	Servicios de ocio y entretenimiento
807 ABM CDU	Servicios profesionales

Asimismo, también se han modificado los precios oficiales que se podrán cobrar al usuario llamante. Dichos precios dependerán de la cuarta cifra (llamada cifra "A") que sigue al número 803, 806 y 807. Los nuevos precios, dependiendo de cual sea el número de la cuarta cifra, serán los siguientes:

P = precio aplicado al abonado llamante.
Valor neto en euros/minuto excluyendo la parte correspondiente al establecimiento de llamada

NXY	803	806	807
A	Acceso desde redes fijas		Acceso desde redes móviles
0 y 1	P ≤ 0,35 €		P ≤ 0,65 €
2 y 3	> 0,35 € hasta 0,75 €		> 0,65 € hasta 1,05 €
4 y 5	> 0,75 € hasta 1 €		> 1,05 € hasta 1,30 €
6 y 7	> 1 € hasta 1,65 €		> 1,30 € hasta 1,95 €
8	> 1,65 € hasta 3,15 €		> 1,95 € hasta 3,45 €
9	P > 3,15 €		P > 3,45 €

Las franjas de numeración y sus bandas de precio asociadas son iguales para los tres códigos (803, 806 y 807) y deberán ser respetadas por todos los operadores.

La nueva numeración 803, 806 y 807 ya debería haber entrado en funcionamiento, pero la CMT aún debe resolver sobre los criterios que aplicará para asignar dicha numeración; por lo que aún no se han otorgado bloques con dicha numeración a ningún operador.

PARA EVITAR SORPRESAS

Póngase en contacto con su operador de telefonía y limite su línea para que no tenga acceso a estas conexiones. Este, es un servicio gratuito que la empresa esta obligada a realizar cuando los usuarios lo soliciten.

Configure su ordenador para limitar el acceso de los menores de edad a deteminadas páginas de contenido para adultos.

Ante cualquier duda, póngase en contacto con la Oficina Municipal de Información al Consumidor OMIC.
Este es un servicio que le ofrece su Ayuntamiento.

Evita concertar citas a través de Internet con personas a las que no conoces.No facilites tu dirección, ni tu número de teléfono, ni el nombre de tu colegio, ni tampoco tu foto.

Desconfía incluso de tus "ciber-amigos", recuerda que las personas con las que estableces contacto a través de la red, no siempre son lo que parecen e incluso puede que no digan la verdad. No olvides que nadie puede verlos.

No todos los lugares de "chat" (charla) a través de la red son apropiados para niños o adolescentes, aún cuando ellos se anuncien como "especiales para niños y adolescentes". Si alguien escribe algo que te resulte vergonzoso, incomodo o que te cause preocupación, informa sobre ello inmediatamente.

No respondas nunca a mensajes obscenos, con fotos indecentes o con contenidos insinuantes. Informa de ellos a tus padres y saca una copia de los mensajes. Podrían ser delictivos.

Te aconsejamos no enviar datos de tu tarjeta de crédito o detalles de tu banco a personas desconocidas, o de las que no has comprobado previamente su identidad. Alguien podría utilizar los datos para robarte.

No facilites tu contraseña a nadie, podrían hacerse pasar por ti.

Desconfía de las ofertas que parecen muy atractivas a primera vista. Lo más probable es que se trate de un engaño.

Permanece alejado de las páginas destinadas a los "mayores de 18 años", esas advertencias están allí para protegerte. Algunas páginas para adultos pueden acarrear costos en tu factura telefónica y descargar la información puede dañar los archivos de su ordenador.