GUÍA DEPROTECCIÓN EN INTERNET

Proceso de Datos en Psicología 2015

CURSO 2014-2015

UNIVERSIDAD DE OVIEDO

COMPONENTES DEL GRUPO

@albertipsikhe
Psicólogo Alberti Psikhe

Emilio Alejandro Alberti Castro

@alvarezpsico
Mónica Álvarez Díaz

Mónica Álvarez Díaz

@psypaulafernand
Psicóloga Paula Fernández

Paula Fernández Fernández

@egainzaRRHH
Elena Gainza Gutiérrez

Elena Gainza Gutiérrez

@mariamoranpsico
María Neir Morán Domínguez

María Neir Morán

@psico_carla
Carla PC

Carla Pantiga Cuesta

@msuarezpsico
MSuárez Psicología

Miriam Suárez Fernández

@patrispsicologa

Patricia Suero Sánchez

@TueroPsicologia
Pelayo Tuero Menéndez

Pelayo Tuero Menéndez

@Psico vanesa
Vanesa PM

Vanesa Pernas Martínez

@psicoconmaria
Psicología con María

María Villar Acebal

@avillegasfpsico
Álvaro Villegas Fuentes

Álvaro Villegas Fuentes

ÍNDICE

1. **Historia de Internet**

2. **Nuevas tecnologías**

    - **Fotos y teléfonos móviles**

3. **Redes sociales**

4. **Ley de protección de datos**

5. **Amenazas y virus**

    - **Tipos de virus informáticos**
    - **Propiedades de los virus informáticos**
    - **Protección**
    - **Antivirus gratuitos y eficaces**

6. **Protección de datos con la presencia de los menores**

7. **El control a través de las Cookies**
    - **¿Qué son?**
    - **¿Qué son las ventanas y elementos emergentes**

8. **Fraudes más comunes en Internet**
    - **Phishing: Fraude en la banca online**
    - **Fraude online: esperar algo que nunca llega**
    - **Pago online: que debes saber para realizar una compra segura**

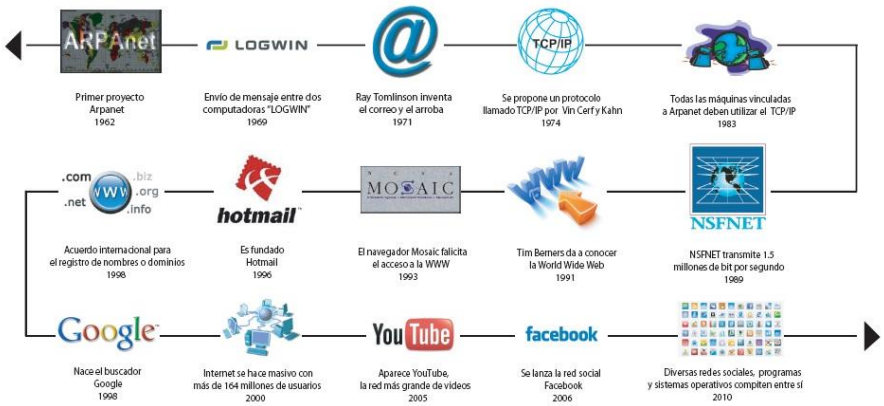
1. HISTORIA DE INTERNET

Los inicios de Internet se remontan a los años 60. Durante la guerra fría, Estados Unidos creó una red exclusivamente militar, con el objetivo de que, en el hipotético caso de sufrir un ataque ruso, se pudiera acceder a la información militar desde cualquier punto del país.

Esta red fue creada en 1969 y se llamó **ARPANET**. En sus inicios, la red contaba con 4 ordenadores distribuidos entre varias universidades del país.

Dos años después, ya se contaba con unos 40 ordenadores conectados. Tal fue el crecimiento de la red que su sistema de comunicación se quedó obsoleto. En este momento dos investigadores crearon el **Protocolo TCP/IP**, que se convirtió en el estándar de comunicaciones dentro de las redes informáticas (actualmente seguimos utilizando dicho protocolo).

Existe una gran controversia a la hora de definir la fecha de nacimiento oficial. Un grupo de autores sitúan este momento en el nacimiento de **ARPANET** en 1969. Este hecho puede considerarse el embrión de internet ya que es el primer intento de unir ordenadores situados en distintos lugares, pero no se puede considerar Internet. La definición más extendida de Internet es la de **Red de redes**. ARPANET no es una red de redes sino unos cuantos ordenadores conectados mediante conexiones telefónicas.



Sería más correcto señalar como el nacimiento de Internet a la puesta en servicio de la red **NSFNET**, una red que ya utiliza los Protocolos TCP/IP y cuya misión es la de ser troncal para la conexión de redes. Esta red se considera una evolución de ARPANET aunque su objetivo es la interconexión de redes usando todos los desarrollos y éxitos de ARPANET.

A partir de ese momento surgieron nuevos formatos:

Podríamos decir que internet tiene 4 usos:

1. Es un **medio de comunicación** que permite compartir ideas hacia todo el mundo a alta velocidad y bajo costo. La mensajería instantánea es uno de los servicios más usados porque permite comunicarse a dos o más personas en tiempo real.
2. **Fuente de información** para uso personal, educativo o comercial. Actualmente internet es la fuente de información más consultada, superando a la televisión, la presa o la radio.
3. **Medio de transacciones y servicios** que permite realizar transferencias, comercio electrónico y movimiento de fondos. Se ha alterado la manera tradicional de trabajar en muchas empresas, muchos trabajadores pueden trabajar desde sus casas, lo que les permite una mayor flexibilidad en términos de horario y localización.
4. **Ocio,** muchas personas, la gran mayoría jóvenes, usan internet para descargar material de la red: películas, series, videojuegos, música, etc. También se puede acceder a una gran variedad de juegos en la red.

En 2014 y por primera vez, el número de usuarios de **Internet en España (76,2%)** ha superado al de las personas que usan **ordenador (73,3%)**. Según una encuesta del Instituto Nacional de Estadística (INE) esta situación se da en todas las Comunidades Autónomas e indica una creciente utilización de otros dispositivos, mayormente smartphones, para la conexión a internet.

El uso de tecnologías en **población infantil (10-15 años)** es muy elevada, el uso de ordenadores con internet alcanza el **92%**. La disposición de teléfono móvil se incrementa significativamente a partir de los **10 años** hasta llegar a un **90,3%** en la población de **15 años.**

En España existen casi **11,9 millones** de hogares con acceso a la red mediante una conexión de banda ancha.

En cuanto al uso de redes sociales, más de la mitad de la población participa en redes sociales como Facebook, Twitter o Tuenti. Los más participativos son los **estudiantes (92%)** y los jóvenes de **16 a 24 años (91,3%)**, mientras que, teniendo en cuenta el sexo, la participación de las **mujeres (68,9%)** es superior a la de los **hombres (65,3%)**

Por otra parte, el porcentaje de personas que compra por Internet ha experimentado una subida de **4,6 puntos** en el último año. Cerca de **14,9 millones** de personas han realizado operaciones de comercio a través de la red alguna vez en su vida.

2. NUEVAS TECNOLOGÍAS

Si bien es cierto que las nuevas tecnologías han supuesto una gran innovación y avance para la humanidad por los múltiples beneficios que ha aportado a nuestra sociedad, pueden llegar a convertirse en nuestro peor enemigo si no las manejamos con la precaución pertinente debido a que nunca antes las nuevas generaciones han tenido a su alcance tanta información y de forma tan rápida como ahora.

Las Nuevas Tecnologías de la Información y las Comunicaciones (NTICs) son un claro distintivo que caracteriza nuestra época actual y se han convertido en herramientas esenciales para las diversas áreas de nuestra vida cotidiana, académica, laboral, social y de ocio. Dentro de las NTICs, además de situar todos los servicios de contacto electrónico, podemos incluir los teléfonos móviles, plataformas online de difusión de contenidos y las redes sociales.

Dejando a un lado los beneficios que han supuesto todas estas nuevas tecnologías, estas mismas pueden suponer un riesgo para la salud, pues pueden hacer que las personas descuiden obligaciones laborales y familiares y llegando a producirse riesgos tales como: aislamiento, pérdida de noción del tiempo, adopción de falsas identidades, acceso a materiales no adecuados y/o perjudiciales, etc.

Los adolescentes parecen ser el colectivo más propenso a sufrir los problemas anteriormente expuestos pues ciertos estudios han recogido que el 85% de este sector tiende a conectarse a Internet y por lo menos alcanzan las más de 5 horas de conexión, siendo el lugar de conexión más habitual su propia casa en al menos el 75% de los casos.

2.1. FOTOS Y TELÉFONOS MÓVILES

La extensión del uso del teléfono móvil ha alcanzado a todos los sectores de la población española, incluidos los más jóvenes. Es frecuente que niños y adolescentes dispongan de teléfono móvil para su uso particular.

La utilización de teléfonos móviles en la adolescencia puede contribuir a desarrollar competencias como la autonomía y la responsabilidad, pero también puede colocar al usuario en situaciones de riesgo: el grado de madurez y desarrollo asociado a la minoría de edad determina que sea un colectivo de especial vulnerabilidad.

Entre los jóvenes españoles la edad media de adquisición del terminal se sitúa entre los 10 y 12 años, y las razones que utilizan los padres e hijos a la hora de justificar el hecho de que se produzca tan pronto son las siguientes: por seguridad, mejor contacto con los amigos y mayor independencia. Son los padres los que se hacen cargo de la factura del teléfono en la gran mayoría de las ocasiones (85,1%).

Según el estudio, los principales usos que los jóvenes dan al teléfono móvil son: para comunicarse, llamadas de voz o mensajes; para acceder a contenidos multimedia, principalmente para escuchar música, ver vídeos o acceder a Internet; como herramienta de ocio; o creación de contenidos, sobre todo fotografías las cuales muchos de ellos también las envían a sus amigos.

El uso excesivo del teléfono móvil puede llevar aparejado un mayor gasto y en casos graves puede conducir a un trastorno de adicción psicológica. Según las encuestas realizadas el 36% de los jóvenes consideraba que realizaba un uso abusivo del teléfono móvil. Las limitaciones que los padres principalmente imponen a sus hijos son el límite de gasto mensual y el acceso a Internet.

Respecto a las amenazas a la privacidad y sexting, el 88,6% de los encuestados admitía realizar fotografías con su terminal, y un 48,2% manifestaba, además, enviarlas a sus contactos.

Una variante al uso del móvil como medio de producción de material multimedia es el sexting que ya se ha comentado anteriormente, y que consiste en realizar fotos o videos personales de

carácter sexy, con más o menos ropa y que luego distribuye de forma voluntaria entre sus amistades a través de bluetooth. Según el estudio 8,1% de los jóvenes admitía haber recibido fotos o videos de chicos de su entorno en posturas provocativas, mientras que el 4% reconocían haber hecho este tipo de fotos o videos, el porcentaje sube en adolescentes de 15-16 años hasta el 6,1%.

En cualquier caso, lo más normal es que las fotos que se realizan con el móvil acaben en la red social de los usuarios por lo que tendríamos asociados los peligros señalados en los puntos anteriores.

Cuando fotografían o graban a otros, el problema está en el hecho de que en muchas ocasiones lo realizan sin permiso, así el estudio refleja que un 17,1% de los jóvenes afirma conocer casos de amigos cuyas imágenes han sido grabadas y difundidas sin permiso.

En cuanto a las consecuencias, cuando se les pregunta a los jóvenes si perciben la difusión de estas imágenes como un problema, mayoritariamente responden que no sobre todo cuando han sido ellos mismos los que han realizados las fotos o videos de ellos mismos. Simplemente manifiesta cierta incomodidad o vergüenza.

Respecto al acceso a contenidos inadecuados, el riesgo radica en el efecto que podría ejercer sobre el menor la visualización de imágenes no apropiadas a su nivel de madurez. El 6,8% de los jóvenes ha accedido a imágenes de contenido sexual o pornográfico, y el 8,4% de ellos han accedido a materiales con contenido racista o violento.

El hecho de recibir en su terminal este tipo de contenidos no es percibido por la mayoría de los casos como un problema, sólo en algunos casos plantean sentir cierta vergüenza o incomodidad.

El ciberbullying puede realizarse de distintas maneras:

- Envío de textos amenazadores.
- Divulgación de imágenes o videos desagradables.
- Realización de llamadas silenciosas insistentes.

El caso de la divulgación de imágenes o videos son más relevantes debido a la rápida y amplia divulgación que se puede realizar de los contenidos y la permanencia de los mismos si se suben a Internet, incluso aunque los contenidos sean retirados en corto intervalo de tiempo (siempre alguien se los ha podido descargar antes de su retirada).

El 5,6% de los menores han recibido mensajes o llamadas de otros menores increpándoles, y un 5% reconoce haber utilizado el móvil para realizar este tipo de llamadas. Otro dato interesante es que el 11,5% ha accedido a imágenes de peleas con personas del entorno. A este fenómeno de grabar agresiones entre menores y colgarlas luego en Internet se le denomina *happy slapping*.

Se aconseja pues una serie de recomendaciones:

a) Sobre configuración del terminal:

- Restringir las llamadas entrantes, es decir, los padres del menor pueden configurar el teléfono para que el menor solo pueda realizar/recibir llamadas a ciertos números.
- Asociar el teléfono móvil del menor al contrato y teléfono de un adulto. De forma que se apliquen filtros de seguridad al teléfono del menor.
- Puede activarse en el teléfono de los padres la opción de localización “GPS” del teléfono móvil del menor.
- Incorporar como configuración predeterminada el bloqueo al acceso de contenidos para adultos.
- Vetar las llamadas anónimas, comerciales y de venta directa en los móviles del menor.

b) Consejos para padres y educadores:

- Dilatar al máximo la edad de posesión del móvil (en la actualidad se sitúa en 10-12 años).
- Acordar junto al menor normas de uso (espacios y tiempos de uso, servicios a los que puede acceder, etc.

- Una buena comunicación entre padres e hijos, en este aspecto es importante que los padres conozcan los riesgos con el fin de que puedan alertar a los hijos sobre los mismos.
- En definitiva, incidir más en la educación de la responsabilidad que en la restricción.

c) Consejos para los menores:

- Respeta las restricciones de uso de la cámara del móvil en ciertos lugares públicos (piscinas, vestuarios,..), no envíes fotos que puedan avergonzarte a tí o otras personas, debes ser consciente de que cuando mandas dichas fotos pierdes el control sobre ellas. Debéis estar atentos que otras personas, especialmente adultos, os tomen fotografías.
- Si te sientes acosado, recibes una imagen de una agresión a otra persona, recibes llamadas o SMS amenazantes guárdalo como prueba y enseñárselo a tus padres, profesor o adulto de confianza.
- Lee atentamente los términos y condiciones de los formularios antes de dar tu número de teléfono, no respondas llamadas o mensajes de desconocidos, ni quedes con personas que has conocido a través del móvil. Si recibes un SMS o MMS que induce a promociones, descargas o accesos a sitios de Internet omítelos.
- Desconecta el bluetooth si no lo estás utilizando y configúralo de forma que no acepte conexiones de dispositivos desconocidos, con el fin de evitar la transferencia de contenidos inapropiados e incluso virus. Si notas algo extraño en el funcionamiento del móvil coméntalo con tus padres.
- Desactiva el sistema de localización (GPS) cuando no te sea necesario.
- En caso de extravío bloquea inmediatamente la tarjeta SIM, para evitar que terceros carguen gastos a tu cuenta.

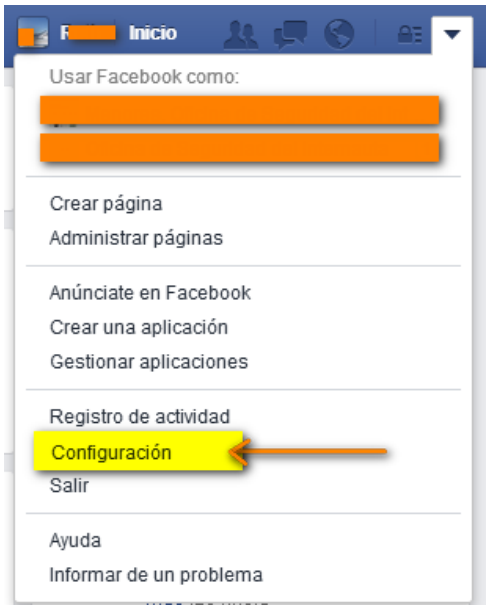
3. REDES SOCIALES

Hoy en día las redes sociales son una parte fundamental de la vida de la mayoría de las personas. Estas ofrecen una multitud de posibilidades que hasta hace unos pocos años eran impensables, el desarrollo ha sido increíblemente rápido y no es fácil para todo el mundo seguir este desarrollo y adaptarnos a él.
Como cualquier herramienta las redes sociales, si no se saben usar bien, tienen sus peligros. La cantidad de información que vertemos al público a través de las redes es tremendo, y la mayoría de veces no somos conscientes de ello: Nombre, dirección, teléfono, amigos, lugares habituales, gustos, intereses, profesión, estudios…

Todas las redes sociales ofrecen una serie de opciones de configuración mediante las cuales podemos controlar la forma en que compartimos nuestra información y con quien, y es responsabilidad de cada uno saber usarlas.

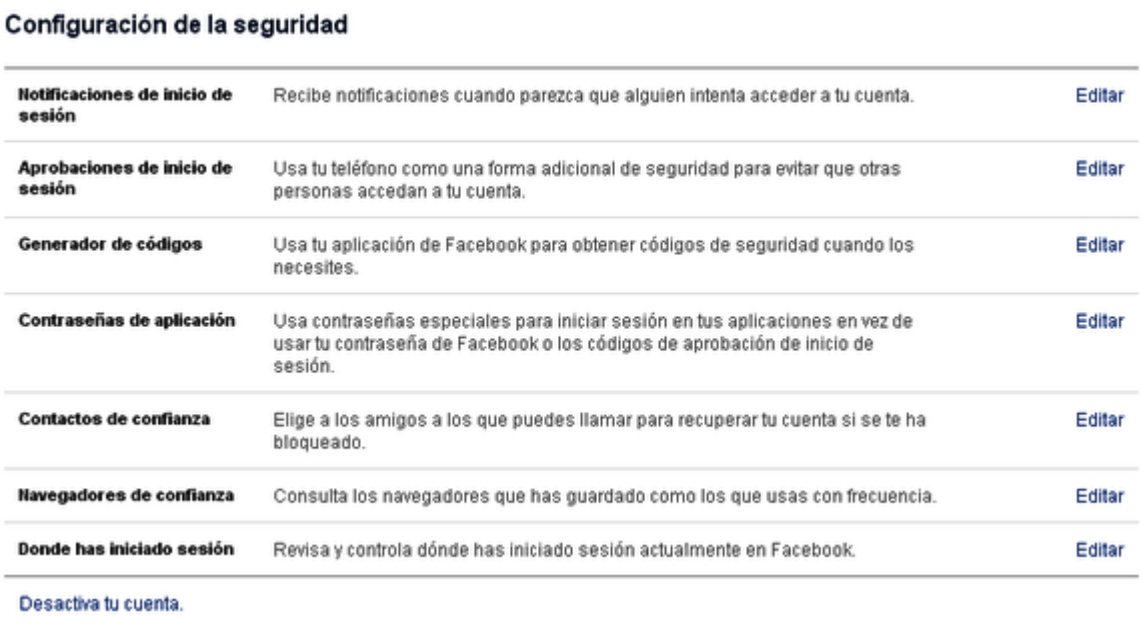
- **Facebook:**

Estas opciones se encuentran disponibles desde la sección ***Configuración***, a la cual se accede desde el menú desplegable situado en la parte superior derecha de la página.



Cuando te das de alta en Facebook, entre los datos que facilitas está tu nombre, correo electrónico y una contraseña. Estos datos puedes modificarlos en cualquier momento desde esta opción. Tu nombre probablemente no cambie, pero puede que en un momento dado, decidas cambiar la cuenta de correo electrónico asociada. Además, la contraseña, siguiendo nuestros consejos de seguridad, debes actualizarla con frecuencia y asegurarte en todo momento que es robusta para evitar que nadie la adivine.

Evita que cualquiera pueda acceder a tu cuenta sin tu consentimiento aplicando todas las medidas de seguridad que Facebook pone a tu disposición: sesiones activas, contraseñas de aplicaciones, aprobaciones de inicio de sesión, etc. Consulta en qué consiste cada función de seguridad y cómo puedes activarlas .



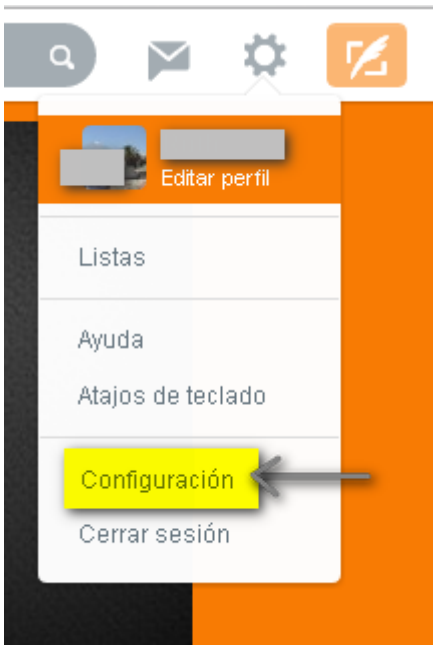
Debes tener siempre muy claro qué tipo de información quieres que cada usuario vea sobre ti. Es decir, ¿quién quieres que vea tus publicaciones? (comentarios, fotos, etc.) o ¿quién puede enviarte solicitudes de amistad? Facebook permite configurar a tu gusto éstas y otras muchas opciones relacionadas con la privacidad . Facebook da las opciones de compartir con todo el **Público**, **solo con Amigos**, o **Solo Yo**, pero además da la opcion de personalizar esta configuración y elegir quienes concretamente

Configuración y herramientas de privacidad

¿Quién puede ver mis cosas?	¿Quién puede ver las publicaciones que hagas a partir de ahora?	**Amigos**	Editar
	Revisa todas tus publicaciones y los contenidos en los que se te ha etiquetado		Usar registro de actividad
	¿Quieres limitar el público de las publicaciones que has compartido con los amigos de tus amigos o que has hecho públicas?		Limitar el público de publicaciones antiguas
¿Quién puede ponerse en contacto conmigo?	¿Quién puede enviarte solicitudes de amistad?	**Amigos de amigos**	Editar
	¿De quién quiero filtrar los mensajes en mi bandeja de entrada?	**Filtrado estricto**	Editar
¿Quién puede buscarme?	¿Quién puede buscarte con la dirección de correo electrónico que has proporcionado?	**Amigos**	Editar
	¿Quién puede buscarte con el número de teléfono que has proporcionado?	**Amigos**	Editar
	¿Quieres que otros motores de búsqueda muestren el enlace de tu biografía?	**No**	Editar

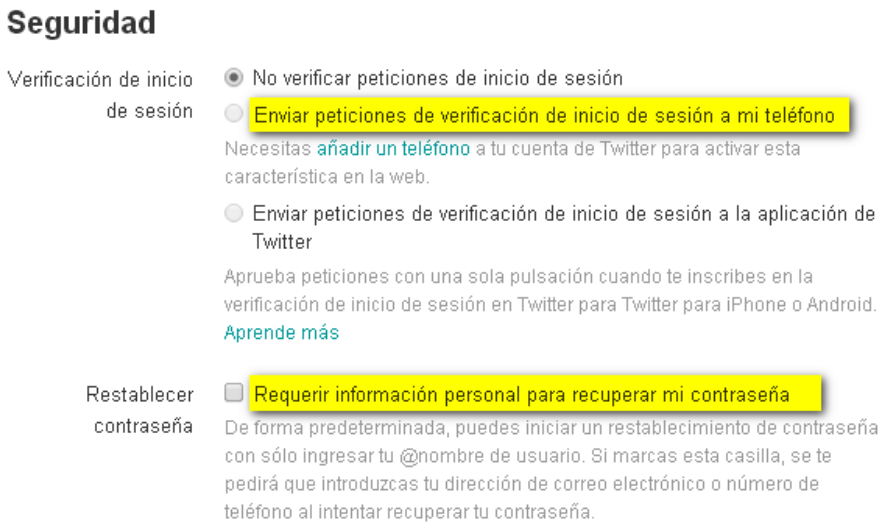
- **Twitter:**

Otra red de gran riesgo es twitter, esta red social también ofrece una serie de opciones de seguridad las cuales se encuentran disponibles desde la sección **Configuración**,a la cual se accede desde el menú desplegable situado en la parte superior derecha de la página.



Cuando te creas una cuenta en Twitter, entre los datos que facilitas está tu nombre de usuario y correo electrónico. Estos datos puedes modificarlos en cualquier momento. También es posible que pida tu numero de telefono.

Para evitar que alguien acceda a tu cuenta sin tu consentimiento aplica todas las medidas de seguridad que Twitter pone a tu disposición: verificación de inicio de sesión, requerimiento de información personal para el restablecimiento de contraseña, etc. Se debe consultar en qué consiste cada función de seguridad y cómo puedes activarlas .



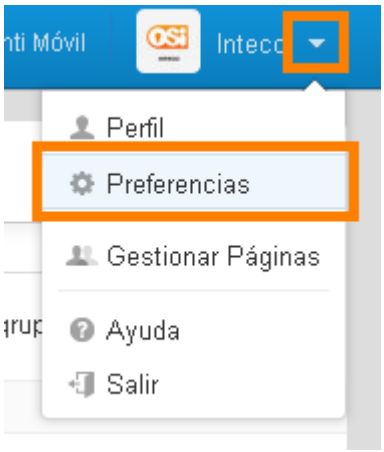
En las opciones de privacidad, Twitter nos permite configurar la privacidad de tus tuits. Si habilitas la opción de **“Proteger mis Tweets”**, sólo las personas que elijas podrán leerlos. Por el contrario, si no lo haces, éstos serán públicos y cualquiera podrá leerlos. Dependiendo del uso que quieras dar a la cuenta de Twitter, deberás tener habilitada una opción u otra.

Una aplicación de terceros es un producto desarrollado por personas ajenas a Twitter y generalmente acceden a tus tuits así como otros datos asociados a tu perfil de Twitter. Te recomendamos que revises las aplicaciones asociadas a tu cuenta y elimines todas aquellas que no utilices o que no sean de confianza .

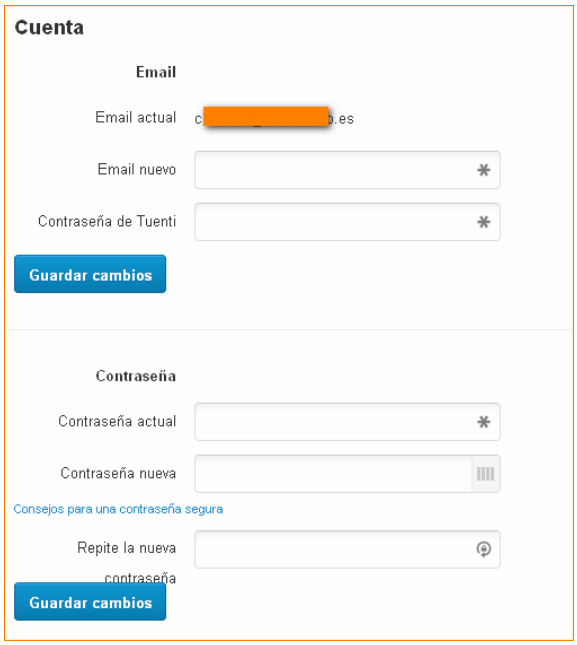
- **Tuenti:**

Tuenti es una red social que suele ser utilizada por usuarios más jóvenes que Facebook, y por ello sus usuarios son más vulnerables. Tuenti ofrece una serie de opciones de configuración que debemos conocer por nuestra seguridad. Puedes acceder a las opciones

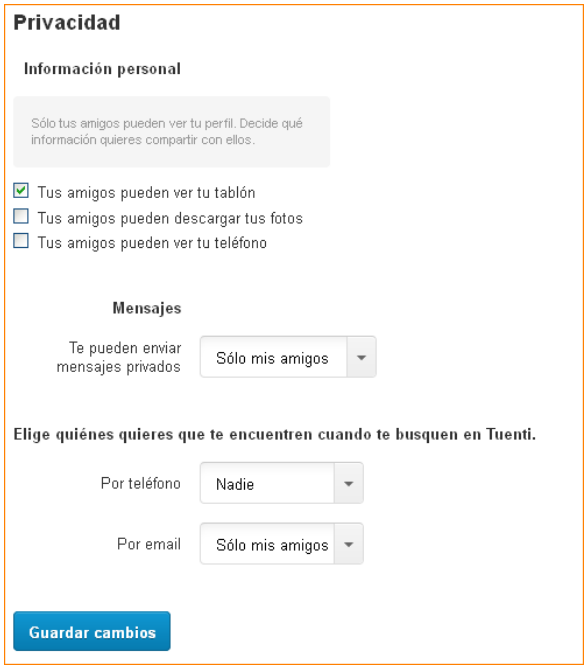
de configuración de la cuenta pulsando en el icono situado en la parte superior derecha de la pantalla, y, a continuación, seleccionando la opción ***Preferencias*.**
La nueva pantalla que se abre contiene un menú en el lateral izquierdo que te redirige a distintas configuraciones. Las opciones más importantes son las que se encuentran en la sección **Privacidad** y **Cuenta**.



Cuando creas una cuenta en Tuenti, los datos que facilitas son tu nombre, correo electrónico y una contraseña.Estos datos puedes modificarlos en cualquier momento desde esta opción. Tu nombre probablemente no cambie, pero puede que en un momento dado, decidas cambiar la cuenta de correo electrónico asociada. Además, la contraseña, siguiendo nuestros consejos de seguridad, debes actualizarla con frecuencia y asegurarte en todo momento que es buena para evitar que nadie la adivine.



Es posible manejar las opciones de privacidad de la forma más sencilla, solo tienes que elegir qué contenidos quieres compartir con tus amigos. Lo más recomendable es activar las opciones más restrictivas: que tus amigos no puedan descargar tus fotos y que no vean tu número de teléfono móvil. Desde esta sección, también elegirás quién puede enviarte mensajes privados.



Es importantísimo **no aceptar «solicitudes de amistad» de personas desconocidas**. Si por la calle no te fías de personas desconocidas, en Internet tampoco. No sabemos quién está detrás de cada cuenta de usuario. Muchas veces una persona se esconde bajo falsos perfiles para engañar a los usuarios. Recuerda que en el momento que aceptas una «solicitud de amistad» tu nuevo amigo podrá ver tu perfil, todas tus fotos, etiquetarte en fotos, escribir comentarios en tu tablón o enviarte mensajes privados. Cuidado con los enlaces que proporcionan algunos comentarios de tu tablón, pueden llevarte a páginas maliciosas o descargar código malicioso en tu ordenador.

Para saber más: https://www.osi.es/es

4. LEY DE PROTECCIÓN DE DATOS

La Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar.

Esta ley se aplica a todos los ámbitos en los que se le requiere información al ciudadano (datos personales, número de teléfono, correo electrónico, comentarios en una red social, fotografías, mensajes enviados mediante aplicaciones, archivos multimedia...) y, hoy en día, nos solicitan información para cualquier actividad (reservar una habitación de hotel, pagos con tarjeta, navegando por internet...).

Estos datos son almacenados en ficheros de información que son administrados por las diversas entidades que requirieron los datos: Administración Pública y empresas privadas.

La información que aportamos contiene datos relevantes sobre nosotros mismos y nuestra vida (quiénes somos, cómo somos, aficiones, gustos, capacidades…), por lo que es necesario que las personas o entidades que los guardan deben protegerlos para garantizar nuestra privacidad. Y debemos conocer cuáles son nuestros derechos respecto a nuestros datos.

El derecho fundamental a la protección de datos es la capacidad que tiene el ciudadano para disponer y decidir sobre todas las informaciones que se refieran a él. Es un derecho reconocido en la Constitución Española y el Derecho Europeo y protegido por la Ley Orgánica de Protección de Datos (LOPD).

4.1 Información y consentimiento.

Hay múltiples formas y vías por las que se requiere la información: contratación telefónica, cumplimentación de un formulario, darse de alta en una red social, imágenes obtenidas mediante una cámara de vigilancia… Antes de ofrecer estos datos, debemos saber por qué, para qué (de forma específica, no se aporta información para finalidades indeterminadas) y cómo van a ser tratados estos datos. Además, es necesario tener información sobre la entidad que recoge esos datos: identidad, dirección, finalidad, tratamiento de los datos...

Cuando contamos con esta información, debemos dar nuestra aprobación para que la entidad o administración pueda recoger y emplear nuestros datos. La Ley permite que se recojan datos sin autorización del usuario cuando se cumpla alguno de los supuestos recogidos en el artículo 6 de la ley (véase Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal).

Salvo casos excepcionales, somos libres de aportar datos relativos a nosotros mismos y siempre tenemos la posibilidad de revocar este consentimiento. Hay datos que son relevantes por la intimidad que suponen, por lo que tienen el consentimiento deberá ser expreso en cuanto a esa información (religión, creencias, ideología, afiliación sindical, salud, origen racial, vida sexual).

TRATAMIENTO DE LOS DATOS: Calidad, seguridad y secreto

En cuanto a la calidad, los datos requeridos deben ser pertinentes para la finalidad planteada, estrictamente necesarios y serán cancelados cuando la finalidad para la que se recogen se vea concluida, y en la recogida de datos, el que los requiere no debe usar engaños no infringir la ley.

El responsable del fichero deberá garantizar la seguridad de los datos. Los datos sólo serán puestos a disposición de personas autorizadas, pudiendo ser recuperados; y serán confidenciales, es decir, el responsable deberá asegurar el carácter secreto de la información.

MIS DERECHOS

El usuario tiene cinco derechos en cuanto a sus datos:

- **Consultar**: quién ha tratado sus datos.
- **Acceso**: conocer el tratamiento de sus datos, la finalidad, el origen de esos datos y comunicaciones realizados o previstas sobre los mismos.
- **Rectificación**: permite corregir errores, modificar los datos que resulten ser inexactos o incompletos y garantizar la certeza de la información objeto de tratamiento.
- **Cancelación**: suprimir los datos considerados inadecuados o excesivos.
- **Oposición**: dirigirse al responsable del encargado de almacenar sus datos. Esto se puede hacer cuando se cumple alguno de estos supuestos: uso de los datos sin consentimiento del usuario, para fines publicitarios o de prospección comercial o cuando el tratamiento tenga por finalidad la adopción de una decisión referida al afectado y basada únicamente en un tratamiento automatizado de sus datos de carácter personal.

QUÉ HACER CUANDO VULNERAN MIS DERECHOS

El usuario que considere que no se han respetado sus derechos conforme a la Ley de Protección de Datos, debe dirigirse la Agencia Española de Protección de Datos. Esta agencia analizará los hechos y, si estima la reclamación, dictará una resolución requiriendo

al responsable del fichero para que haga efectivo el derecho de que se trate en un plazo determinado. La ley considera los siguientes tipos de infracciones:

- **Leves** (sanción entre 900 a 40.000 euros): no remitir a la Agencia Española de Protección de Datos las notificaciones previstas en esta Ley o en sus disposiciones de desarrollo, no solicitar la inscripción del fichero de datos de carácter personal en el Registro General de Protección de Datos, el incumplimiento del deber de información al afectado acerca del tratamiento de sus datos de carácter personal cuando los datos sean recabados del propio interesado y la transmisión de los datos a un encargado del tratamiento sin dar cumplimiento a los deberes de esta Ley.
- **Graves** (sanción entre 40.001 a 300.000 euros): iniciar la recogida de datos de carácter personal, sin autorización de disposición general; tratar datos de carácter personal sin recabar el consentimiento de las personas afectadas, tratar datos de carácter personal o usarlos posteriormente con conculcación de los principios y garantías establecidos en el artículo en la presente Ley; la vulneración del deber de guardar secreto acerca del tratamiento de los datos de carácter personal ; el impedimento o la obstaculización del ejercicio de los derechos de acceso, rectificación, cancelación y oposición; el incumplimiento del deber de información al afectado acerca del tratamiento de sus datos de carácter personal cuando los datos no hayan sido recabados del propio interesado; el incumplimiento de los restantes deberes de notificación o requerimiento al afectado; mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad; no atender los requerimientos o apercibimientos de la Agencia Española de Protección de Datos o no proporcionar a aquélla cuantos documentos e informaciones sean solicitados por la misma; la obstrucción al ejercicio de la función inspectora y la comunicación o cesión de los datos de carácter personal sin legitimación.
- **Muy graves** (sanción desde 300.0001 a 600.000 euros): La recogida de datos en forma engañosa o fraudulenta, tratar o ceder los datos de carácter personal, no cesar en el tratamiento ilícito de datos de carácter personal cuando existiese un previo requerimiento del Director de la Agencia Española de Protección de Datos para ello.

TRATAR LOS DATOS DE OTRAS PERSONAS

- Cuando informamos sobre algún aspecto o damos información sobre una persona pública debemos ser respetuosos con la dignidad de las personas objeto de nuestras críticas.

- Si se publica información sobre alguien, tener el consentimiento de dicho usuario para hacer uso de esos datos de forma pública.
- Tenemos que tener cuidado en cuanto a la plataforma elegida para publicar información, ya que, con el uso de cierta información (imágenes, vídeos) podemos incurrir en responsabilidad en materia de protección de datos personales.
- Debemos ser cautelosos en el uso de información que puede escapar a nuestro control en la red.
- Mantener cautela con cierta información que pueda poner en riesgo la integridad de menores o personas con discapacidad.
- Cuidar que la información publicada esté contrastada.
- Retirar información referida a una persona cuando ésta lo requiera.

5. AMENAZAS Y VIRUS

VIRUS INFORMÁTICOS. Tipos

- **Malware infeccioso**

  - ***Virus***

Un virus informático es un programa de ordenador que puede infectar otros programas, modificándolos para incluir una copia de sí mismo. Al ejecutarse, se propaga infectando otros softwares ejecutables dentro de la misma computadora

  - ***Gusanos***

Un gusano es un programa que se transmite a sí mismo, explotando vulnerabilidades en una red de computadoras para infectar otros equipos. El principal objetivo es infectar a la mayor cantidad posible de usuarios, y también puede contener instrucciones dañinas al igual que los virus.

- **Malware oculto**

  - ***Backdoor***

Es un método para eludir los procedimientos habituales de autenticación al conectarse a una computadora.Pueden instalarse previamente al software malicioso para permitir la entrada de los atacantes.Para instalar puertas traseras pueden usarse troyanos, gusanos u otros métodos.

  - ***Drive-by downloads***

Una de cada 10 páginas web que han sido analizadas a profundidad puede contener los llamados *drive by downloads*, que son sitios que instalan spyware o códigos que dan información de los equipos sin que el usuario se percate.

- ***Rootkits***

Las técnicas conocidas como rootkits modifican el sistema operativo de una computadora para permitir que el malware permanezca oculto al usuario. Por ejemplo, los rootkits evitan que un proceso malicioso sea visible en la lista de procesos del sistema o que sus ficheros sean visibles en el explorador de archivos. Este tipo de modificaciones consiguen ocultar cualquier indicio de que el ordenador está infectado por un malware.

- ***Troyanos***

Son programas maliciosos que están disfrazados como algo inocuo o atractivo, y que invitan al usuario a ejecutarlo ocultando un software malicioso.Este software puede tener un efecto inmediato y acarrear muchas consecuencias indeseables, por ejemplo, borrar los archivos del usuario o instalar más programas indeseables.

- **Malware para obtener beneficios**

  - **Mostrar publicidad**

    - ***Spyware***

    Se trata de archivos o aplicaciones que son instalados en los sistemas, algunas veces sin autorización de los usuarios, otras veces después de que acepten las "Condiciones de Uso". Estos archivos se ejecutan en segundo plano, cuando los usuarios se encuentran conectados a Internet. Los Spyware monitorizan lo que hacen los usuarios, y envían la información hacia servidores que almacenarán los datos para fines comerciales, delictivos... Dicha información se vende a ciertos proveedores de productos o servicios, que posteriormente bombardearán los buzones de correo electrónicos de los usuarios con molestos e-mails que ofrecen viajes, créditos, sorteos…

    - ***Adware***

    Muestran publicidad al usuario de forma intrusiva en forma de ventana emergente *(pop-up)* o de cualquier otra forma. Esta publicidad aparece inesperadamente en el equipo y resulta muy molesta.

- **Robar información personal**

Los keyloggers y los stealers son programas maliciosos creados para robar información sensible. El creador puede obtener beneficios económicos o de otro tipo a través de su uso o distribución en comunidades underground. La principal diferencia entre ellos es la forma en la que recogen la información:

  - ***Keyloggers***

Monitorizan todas las pulsaciones del teclado y las almacenan para un posterior envío al creador. Por ejemplo al introducir un número de tarjeta de crédito el keylogger guarda el número, posteriormente lo envía al autor del programa y este puede hacer pagos fraudulentos con esa tarjeta.

  - ***Stealers***

También roban información privada pero solo la que se encuentra guardada en el equipo. Al ejecutarse comprueban los programas instalados en el equipo y si tienen contraseñas recordadas, por ejemplo en los navegadores web o en clientes de mensajería instantánea, descifran esa información y la envían al creador.

- **Realizar llamadas telefónicas**

  - ***Dialers***

Los dialers son programas maliciosos que toman el control del módem, realizan una llamada a un número de teléfono de tarificación especial (a veces internacional) y dejan la línea abierta cargando el coste de dicha llamada al usuario infectado. La forma más habitual de infección suele ser en páginas web que ofrecen contenidos gratuitos pero que solo permiten el acceso mediante conexión telefónica. Suelen utilizar como señuelos videojuegos,salvapantallas, pornografía u otro tipo de material.

- **Ataques distribuidos**

- ***Botnets***

Un "bot" es un tipo de programa malicioso que permite a un atacante tomar el control de un equipo infectado. Por lo general, los bots, también conocidos como "robots web" son parte de una red de máquinas infectadas, conocidas como “botnet”, que comúnmente está compuesta por máquinas víctimas de todo el mundo.

PROPIEDADES DE LOS VIRUS INFORMÁTICOS

De la misma manera que los ordenadores fueron creados a imagen del ser humano (memoria humana versus RAM, cerebro versus CPU…), los que diseñan virus informáticos buscan una semejanza con los virus orgánicos que atacan al ser humano:

1. **Auto-reproducción:**

   Los virus informáticos tipo “gusano” se autorreplican para infectar cada vez más número de archivos “sanos” lo más rápidamente posible.

2. **Migración:**

   En un ordenador, el medio de propagación a otras zonas son los USB, los discos, el correo electrónico… Así, puede llegar a otras localizaciones físicas.

3. **Resistencia parcial:**

   Del mismo modo que algunos virus humanos pueden mutar su código genético para evadir la acción de las vacunas, los virus informáticos pueden aislarse o instalarse en la memoria del aparato para que el antivirus no pueda eliminarlos.

4. **Acción destructiva:**

   Elimina datos, roba información, daña el disco duro… En el peor de los casos inutilizará el aparato completamente, dejándolo completamente fuera de nuestro control.

PROTECCIÓN

- **Firewall:**

Prohíbe el acceso de intrusos al equipo cuando la persona está conectada a internet. El usuario puede configurar qué programas acceden al ordenador.

- **Antivirus:**

Son programas especializados en detectar y eliminar los virus informáticos en todas sus formas. Sin embargo, no implican protección frente a otros tipos de malware como el Spyware o el Adware.

- **Antimalware:**

Los programas anti-malware son más genéricos que los antivirus, y ejercen su acción no solamente sobre virus informáticos sino también sobre otros tipos de amenazas. Pueden combatir el malware de dos formas:

1. Proporcionando protección en tiempo real (real-time protection) contra la instalación de malware en una computadora. El software anti-malware escanea todos los datos procedentes de la red en busca de malware y bloquea todo lo que suponga una amenaza.
2. Detectando y eliminando malware que ya ha sido instalado en una computadora. Este tipo de protección frente al malware es normalmente mucho más fácil de usar y más popular.

Antivirus gratuitos y eficaces:

1.Avast! Free Antivirus

Es un antivirus gratuito que no sólo cuenta con versión para Windows, sino que también dispone de una para equipos con sistema operativo Linux. Ofrece los niveles de protección básica para un ordenador: antivirus y antispyware. Gracias a ellos no sólo podrás librarte de los virus, sino también de los programas que se instalan en tu equipo de forma silenciosa y se encarguen de espiar lo que haces.

2. AVG Antivirus Free 2013

Protección contra los virus y el malware para tu PC. Está disponible para el sistema operativo Windows y sus bases de datos de virus se actualizan cada cierto tiempo. Los análisis se ejecutan con cierta lentitud pero es uno de los antivirus gratuitos que menos consumo de memoria RAM requiere.La tasa de detección de virus y demás malware es bastante alta, y ofrece protección web, antiphising y antispyware.

3. Avira Free Antivirus

Entre las amenazas de las que puede proteger tu equipo están los virus, los rootkits, los gusanos y los troyanos. Este sistema de protección ofrece una muy buena tasa de detección y bloqueo, dejando pasar muy pocas muestras. Destaca por su modo de ejecución, muy silencioso y rápido, con un consumo de recursos escasos. El punto negativo es que cuenta con un panel de administración un tanto complejo para los principiantes.

4. Windows Defender

Destaca en lo que se refiere a la detección de virus en archivos comprimidos, tanto online como offline, donde se postula como uno de los mejores en este sentido. Sus carencias están en la parte de funciones y diseño, presentando una interfaz y panel de control un tanto anticuado y demasiado sencillo.

5. Bitdefender

No cuenta con sistema de protección antispyware, antiphising, ni protección web. Sin embargo, en cuanto al bloqueo de infecciones y la detección de virus es de lo mejor que hay, ofreciendo una alta y eficaz respuesta tanto online como offline, en archivos comprimidos, unidades extraíbles y demás.

6. Panda Cloud Antivirus Free

Ofrece una interfaz bastante sobria y sin complicaciones, con muy pocos menús. Se trata de un antivirus gratuito muy ligero y rápido al no necesitar actualizaciones.Sin embargo, no permite programar los análisis ni tiene protector web.

7. PC Tools

El escaneo es muy rápido y busca virus en la memoria, discos y carpetas de correo del equipo, aunque su nivel o fuerza de detección es menor al resto de antivirus de esta lista. Hay que tener en cuenta que no permite realizar análisis por carpetas, sólo ofrece la opción de análisis completos.

8. Ad Aware Free Antivirus

Detecta y elimina cualquier tipo de virus, programa espía, adware o troyano. Su uso es relativamente sencillo, con varios botones desde la pantalla principal para configurarlo adecuadamente. Podrás analizar por separado algunas partes del PC y otras no, para ahorrar en el consumo y rendimiento de tu PC mientras trabaja en segundo plano.

ALGUNOS CONSEJOS…

- Tener el sistema operativo y el navegador web actualizados.
- Tener instalado un antivirus y un firewall y configurarlos para que se actualicen automáticamente, ya que cada día se crean nuevas amenazas.
- Utilizar una cuenta de usuario con privilegios limitados, la cuenta de administrador solo debe utilizarse cuando sea necesario cambiar la configuración o instalar un nuevo software.
- Tener precaución al ejecutar software procedente de Internet o de algún medio extraíble (CD, USB…). Es importante asegurarse de que proceden de algún sitio de confianza.
- En tablets, teléfonos móviles y otros dispositivos portátiles, es recomendable instalar aplicaciones de tiendas muy reconocidas, como App Store, Google Play o Nokia Store, pues esto garantiza que no tendrán malware. Existe, además, la posibilidad de instalar un antivirus para este tipo de dispositivos.
- Evitar descargar software de redes P2P, ya que realmente no se sabe su contenido ni su procedencia.
- Permitir *JavaScript, ActiveX y cookies* sólo en páginas web de confianza.
- Utilizar contraseñas de alta seguridad.
- Es muy recomendable hacer copias de respaldo regularmente de los documentos importantes a medios extraíbles como CD, DVD o Disco duro externo, para poderlos recuperar en caso de infección por parte de algún malware, pero solamente si se esta 100% seguro que esas copias están limpias.

6. Protección de datos (páginas web, redes sociales, juegos, mensajería instantánea) con la presencia de menores.

Un estudio reciente, respecto al uso de Internet, ha considerado que el 72% de los niños entre 11 y 14 años cuentan con un perfil al menos en las redes sociales, a pesar de ser algo ilegal, pues la edad mínima establecida en España son los 14 años. Además, el 40% de los padres no supervisa el uso que hace su hijo de Internet. Algunos riesgos a los que se exponen son:

- **Proporcionar sus datos personales:** solemos advertir que no den ningún dato (incluidas fotos) que les identifique a desconocidos. Tampoco cuando se registran en una web.
- **Chantajes y abusos:** delincuentes aprovechan la información proporcionada por la víctima para chantajearla. Por ejemplo, la **sextorsión** es un tipo de chantaje donde se pide dinero a cambio de no divulgar el desnudo de la víctima.
- **Contenido inapropiado:** Internet nos permite acceder a una cantidad ingente de información. Información que no siempre es la adecuada para su edad, ya sea voluntaria o involuntariamente. Debemos enseñar a nuestros hijos a distinguir el contenido de calidad y bloquear el acceso a aquello que pueda ser perjudicial.
- **Ciberadicción o trastorno de adicción a Internet (IAD):** trastorno que se caracteriza por el uso excesivo, patológico y problemático de la red.

Por ello, es imprescindible que los padres fomenten un consumo responsable del Internet y las nuevas tecnologías en sus hijos. A continuación se plantea una especie de guía para que puedas enseñarle a tus hijos cómo usar correctamente Internet.

1. **Evitar contenidos inapropiados.**

Para evitar que los niños entren en páginas con contenido poco apropiado para su edad, hay varias opciones; instalar un navegador específico o utilizar un software de control

parental (limitan y controlan el uso de Internet realizada por los niños) junto con el navegador habitual. Algunos ejemplos de software de control parental son;

- **Verity:** su instalación es gratis y permite supervisar y hacer un seguimiento de las actividades de los niños en el ordenador cuando están o no en línea, sin invadir su espacio.
- **Control Kinds:** este programa filtra todos los sitios web con contenido inapropiado, es compatible con todos los navegadores y está protegido con una contraseña entre varias de sus cualidades.
- **Kidbox:** es gratuito y se puede utilizar para ordenadores y dispositivos móviles. Ejerce un control del uso del ordenador mediante la cantidad de horas y la franja horaria utilizada, historial con todos los vídeos , juegos y páginas utilizadas, y también realiza un seguimiento semanal de los contenidos a los que ha accedido el niño.
- **Qustodio** (http://qustodio.softonic.com/)
- **Weblocker** (http://weblocker.softonic.com/)
- **Golden Filter Premium** (puedes descargarlo aquí: http://www.osi.es/herramientas-gratuitas?herramienta_selec[]=406)
- **Prot-on** (puedes descargarlo aquí: http://www.osi.es/herramientas-gratuitas?herramienta_selec[]=406)
- **Instrucciones de Windows para activar el Control parental:**

Para activar el Control parental para una cuenta de usuario estándar

1. Para abrir Control parental, haga clic en el botón **Inicio**, después en **Panel de control** y, a continuación, en **Cuentas de usuario y protección infantil**, haga clic en **Configurar el Control parental para todos los usuarios**. Si se le solicita una contraseña de administrador o una confirmación, escriba la contraseña o proporcione la confirmación.

2. Haga clic en la cuenta de usuario estándar para la que desea establecer el Control parental. Si la cuenta de usuario estándar no está aún configurada, haga clic en **Crear nueva cuenta de usuario** para configurar una cuenta nueva.

3. En **Control parental**, haga clic en **Activado, aplicar configuración actual**.

4. Una vez que haya activado el Control parental para la cuenta de usuario estándar de un niño, puede ajustar los siguientes valores individuales que desea controlar:

   - **Límites de tiempo.** Puede establecer límites temporales para controlar el momento en que los niños pueden iniciar una sesión en el equipo. Los límites de tiempo impiden que los niños inicien una sesión durante las horas especificadas. Puede establecer distintas horas de inicio de sesión para cada día de la semana. Si hay una sesión iniciada cuando finalice el tiempo asignado, se cerrará automáticamente. Para obtener más información, consulte Controlar el momento en que los niños pueden usar el equipo.
   - **Juegos.** Puede controlar el acceso a los juegos, elegir una clasificación por edades, elegir los tipos de contenido que desea bloquear y decidir si quiere permitir o bloquear juegos específicos. Para obtener más información, consulte Elegir juegos aptos para niños.
   - **Permitir o bloquear programas específicos.** Puede impedir que los niños ejecuten programas que no quiera que ejecuten. Para obtener más información, consulte Impedir que los niños usen programas específicos.

2. Utilizar navegadores específicos.

Es posible instalar un navegador específicamente para niños, en lugar de utilizar los generales como Internet Explorer o Mozilla. Entre estos navegadores para los menores destacan ; Magic Desktop de Easybits o Kids Browser de Kidrocket, que sólo permiten el acceso a unas páginas determinadas. Como inconveniente de estos navegadores es que la

navegación queda muy limitada, por lo que son adecuados para niños hasta 10 años de edad.

3. Consejos para una navegación segura.

Aunque haya instalado software de control parental:

- Procure no dejar solos a los niños mientras navegan y proteja el ordenador con una clave para evitar que lo arranquen sin su presencia.
- Instale el ordenador en una habitación común, no en el cuarto del niño. Así, será más fácil controlar lo que está haciendo y cuánto tiempo lo utiliza.
- Consulte las páginas de la UE dedicadas a protección de menores en Internet.
- Si encuentra contenidos ilegales (pedofilia, terrorismo, etc.) mientras navega, presente una denuncia en **www.protegeles.com.**
- Ofrécele una l**ista de sitios** que le resulten **interesantes**. Así evitaremos que divague por la Red con consecuencias impredecibles.
- **Revisión** de las páginas que ha visitado usando el **historial del navegador**.

4. No compartir información personal.

Controla los datos personales que solicitan las páginas infantiles para niños y presta atención a aquellas que piden información personal. Habla con tu hijo para hacerle ver los peligros que tiene facilitar determinados datos de forma pública. Adviértele también ante los sorteos y promociones estafa y recuérdale que nadie le va a regalar algo porque sí o sólo por introducir sus datos personales.

5. Enlaces desconocidos.

Es frecuente recibir enlaces a través del correo electrónico o en redes sociales en los que nos invitan a pulsar para recibir una información determinada. Es aconsejable avisar al niño de que no pulse sobre ningún link cuya procedencia no resulte conocida, y que siempre pregunte a un mayor antes de hacerlo.

6. Limita las descargas.

Los juegos, la música gratuita, las barras de herramientas animadas, las aplicaciones infantiles y otras descargas a priori atractivas para los niños pueden llenar tu ordenador de spyware o software malicioso. Dependiendo de la edad del niño se le puede enseñar que no debe bajar nada de fuentes no fiables en Internet o pedirle que no descargue nada sin el consentimiento de un adulto.

7. Uso de chats y programas de mensajería.

Los chats, las redes sociales y los servicios de mensajería instantánea pueden ser canales que los niños utilicen para compartir intereses y consolidar sus amistades. Sin embargo, el anonimato de Internet puede poner a los más pequeños en peligro de ser víctimas de impostores. Para minimizar su vulnerabilidad, enséñales a tomar este tipo de precauciones:

1. Usar siempre un nick para identificarse, no su nombre persona
2. Nunca proporcionar el número de teléfono o dirección
3. Nunca enviar fotografías suyas
4. Nunca quedar con alguien a quien no conoce

8. Uso de redes sociales.

Si aún así tus hijos utilizan Facebook o cualquier otra red, explícales correctamente los riesgos que implica y recuérdales que no compartan información personal ni aceptan amistad de personas que no conocen. Ayúdales a configurar la privacidad de su perfil.

Para saber más…

- http://www.infanciaytecnologia.com/
- http://www.pantallasamigas.net/
- http://www.internetamiga.net/

Consejos generales de seguridad para todos los usuarios:

1. Elige contraseñas diferentes para cada servicio de Internet.
2. Cámbialas con frecuencia.
3. Cambia la contraseña que viene por defecto del Wi-fi doméstico
4. Actualiza tu sistema operativo y tu navegador.
5. Verifica de forma regular los movimientos de tu cuenta bancaria.
6. Haz tus compras o transacciones siempre desde el mismo dispositivo.
7. Instale un antivirus.
8. Desconfía de los mensajes que adjunten enlaces.
9. Evita la ejecución de archivos sospechosos.
10. Descarga aplicaciones desde los sitios web oficiales.
11. Acepta únicamente a los contactos que conozcas.

Enlaces interesantes:

- https://www.gdt.guardiacivil.es
- http://www.osi.es/
- http://www.aui.es/

¡Mide tus conocimientos sobre la seguridad en la Red!

- http://www.osi.es/es/cuanto-sabes

Mitos sobre seguridad en Internet, ¿sabrías diferenciar la información verdadera de la falsa?

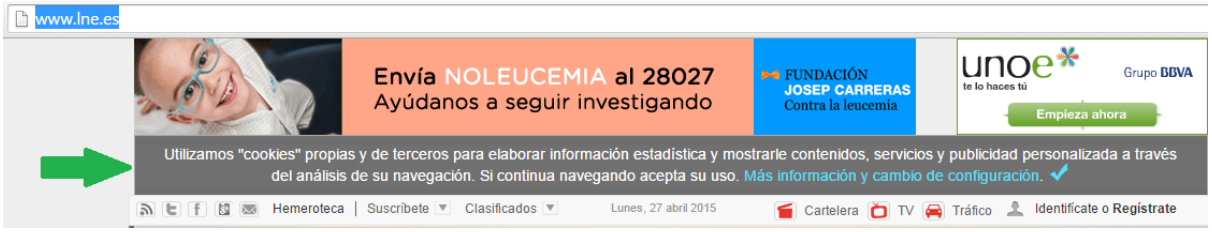
- http://www.osi.es/es/test-evaluacion/mitos-sobre-seguridad-en-internet-verdaderos-o-falsos

7. El control a través de las Cookies

Las **cookies** son pequeños archivos de texto, que pueden estar encriptados, que se almacenan en el navegador web del usuario que accede a una página web. Es importante señalar que las cookies no pueden modificar información en el ordenador del usuario. Tienen varias funciones, mientras que algunas de ellas tienen el objetivo de facilitar la navegación, otras pueden tener fines más perversos.
Su principal función es **autentificar al usuario** en diferentes páginas dentro de la misma, es decir, si eres suscriptor de un periódico e introduces tu usuario y contraseña al inicio, no se te pedirá en cada noticia. El servidor también utiliza las cookies de sesión para almacenar información sobre la actividad del usuario en la página, para que los usuarios puedan volver con facilidad al lugar donde abandonaron las páginas del servidor. Por defecto, las páginas web no tienen en realidad ningún tipo de "memoria". Las cookies le dicen al servidor qué páginas mostrar para que el usuario no tenga que recordarlas o volver a empezar a navegar por todo el sitio hasta encontrar donde se quedó.
Las cookies también se pueden utilizar para conocer los **hábitos de navegación** del usuario, violando su privacidad en favor de agencias de publicidad.

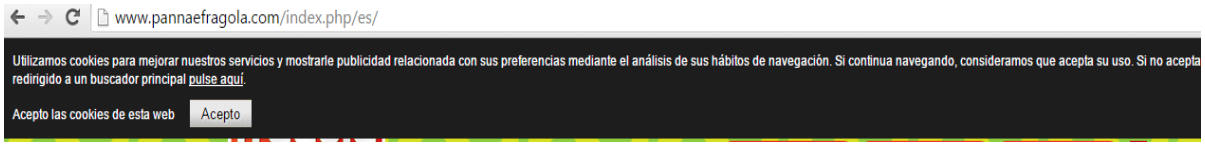
Algunas de las operaciones que se pueden realizar mediante *cookies* también se pueden hacer mediante otros mecanismos (IP, query string, etc). Sin embargo, estas alternativas a las *cookies* tienen sus propios inconvenientes, lo que hace que las *cookies* sean la opción preferida en la práctica.

Dado que la protección de la privacidad está muy valorada y es un derecho de todo usuario de internet, vale la pena estar protegido frente a las amenazas que las cookies pueden plantear. Puesto que las cookies transmiten información entre el navegador y el sitio web, si un enemigo o una persona no autorizada se interpone en la transmisión de datos, la información recibida por las cookies puede ser interceptada y utilizada con fines diferentes a los originales.
Otros ataques relacionados con las cookies están vinculados con la explotación de configuraciones defectuosas de cookies en los servidores. Los atacantes desviarán entonces los datos delicados para fines indeseados.
Debido a su flexibilidad y al hecho de que muchas de las webs más grandes y visitadas utilizan cookies por defecto, las cookies son prácticamente inevitables. Desactivar las cookies haría que un usuario no pudiera acceder a la mayoría de los sitios usados de forma masiva en internet, como YouTube, Gmail, correo Yahoo y otros. Incluso los buscadores necesitan las cookies para los ajustes de idioma.

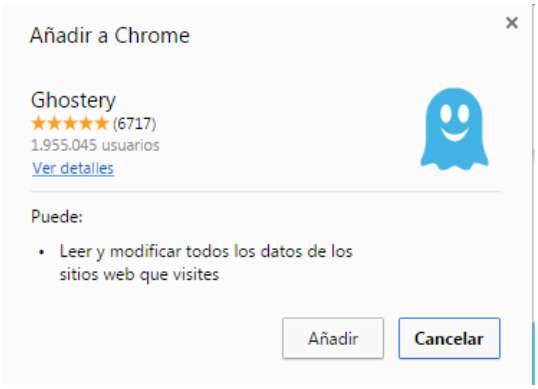


Ejemplo de aviso de cookies en una página.

En este caso, por ejemplo, no nos piden que las aceptemos, sino que su aceptación está implícita en el uso de la página. En otras webs, se pide al usuario que acepte, indicando que, si no lo hace, será redirigido a otra página puesto que su navegación no será posible. Este es el caso del siguiente ejemplo.

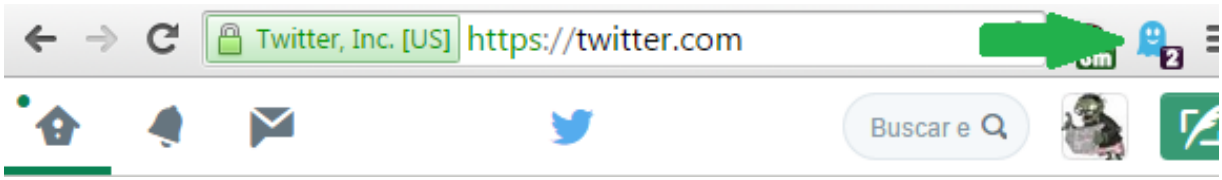


Herramienta para evitar ser rastreados a través de las cookies

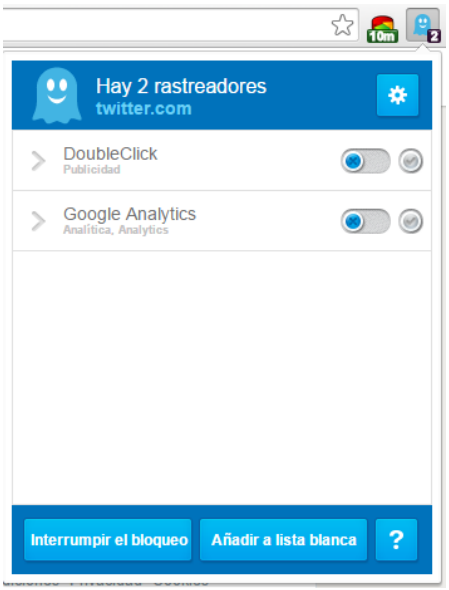


Aunque el uso de cookies sea inevitable, permitir que otros obtengan información sobre nosotros a través de ellas puede ser solucionado con la instalación de algunas aplicaciones en nuestro navegador web. Una de ellas, de uso gratuito, es Ghostery.

Ghostery es una extensión para Google Chrome que puede ser instalada desde su página web: https://www.ghostery.com/es/home. Esta aplicación se mantendrá activa mientras navegamos y nos avisará de los motores de búsqueda que están rastreando nuestra actividad en esa página web, dándole la opción al usuario de bloquear esos rastreadores, de forma que pueda decidir quién puede acceder al rastro que deja en internet y quién no.



Una vez que tengamos la aplicación instalada, veremos el icono del fantasma a la derecha de nuestro navegador.



Junto al icono, aparecerá un número, que nos indica el número de rastreadores que existen en esa página en ese momento. Por ejemplo, podemos ver que en twitter.com existen dos rastreadores. Si hacemos clic en el icono, se ofrecerá una lista detallada de ellos. Con hacer clic en el círculo azul que aparece junto al rastreador, lo deshabilitaríamos.

Junto a cada rastreador, aparece una breve descripción de él, para que podamos saber qué estamos bloqueando.

En la página de La Nueva España, aparecen más rastreadores. Al entrar en la página, aparece una lista de ellos en un recuadro morado abajo a la derecha. Podemos, una vez conocida la lista, abrir la aplicación y bloquear aquellos que nos interesen. Es importante recordar que, una vez bloqueados, hay que volver a cargar la página para que los cambios surtan efecto.

- **¿Qué son las ventanas y elementos emergentes?**

Las ventanas emergentes o *"pop-ups"* son ventanas adicionales que se abren cuando se visitan algunas páginas web. En unos casos pueden ser legítimas e inofensivas, pero en otros (desgraciadamente la mayoría) pueden contener anuncios o presentar ofertas especiales tras las cuales se puede ocultar la instalación de un software malicioso, un virus que nos hará la vida imposible.
Hay diferentes formas de hacer frente a esta amenaza, por suerte bastante variadas y accesibles. A continuación un resumen rápido de todas ellas.

Herramientas para bloquear las ventanas y elementos emergentes

Se podría decir que estas herramientas se "enfrentan" ante el peligro desde 4 posibles frentes, todos ellos con garantías, a disponibilidad del usuario está el elegir cuál prefiere:

1. Desde la configuración del PC
2. Desde la configuración del navegador
3. Desde una extensión al navegador
4. Desde un programa específico

Desde la configuración del PC

En el caso de que tengas un sistema operativo de Windows, sigue este itinerario:
Inicio -> Panel de Control -> Opciones de Internet -> Privacidad -> activa la opción de "bloquear ventanas de aparición instantánea" -> Haz click en "Configuración" y activa el nivel del Filtro hasta su configuración más alta. Cierra la pestaña de Configuración y haz click en "Aplicar" el cambio de Privacidad.

Desde la configuración del navegador

- En Internet Explorer: Herramientas ->Opciones ->Privacidad y marca la opción de "Bloquear ventanas automáticas"
- En Google Chrome: En teoría debería estar marcado por defecto, si no lo estuviera, sigue este itinerario: Configuración ->Configuración avanzadas ->Configuración de contenido -> marca el cuadro de "No permitir las ventanas de aparición automática de ningún sitio".
- En el Safari de Apple: Safari -> Preferencias ->Seguridad -> Selecciona la opción de "Bloquear las ventanas de aparición automática".
- En Mozilla Firefox. como en Chrome, debería estar activado, pero por si acaso, asegúrate: Firefox ->Preferencias ->Contenido -> marca la opción de "Bloquear ventanas de aparición automática".

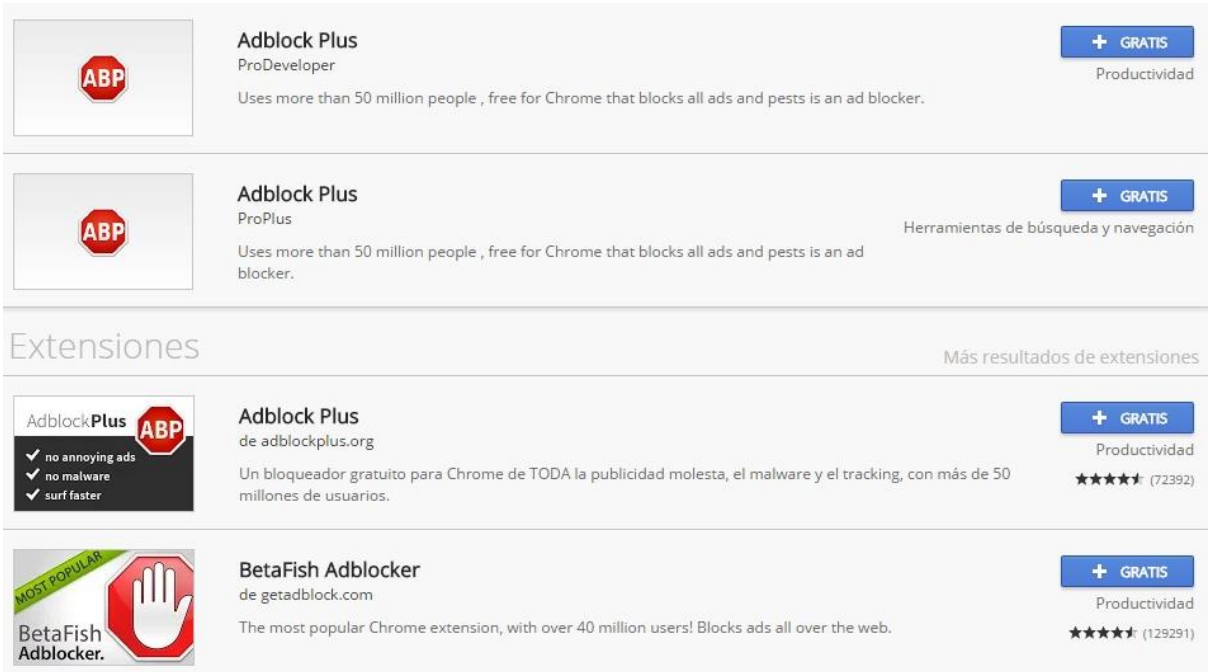
Desde una extensión del navegador

Las extensiones son "aplicaciones" que se le pueden añadir a los navegadores que tienen funcionalidades específicas no incluidas por defecto en el navegador y que puedes añadir fácilmente y gratuitamente la mayoría de los casos y te aportarán una mayor y mejor experiencia de navegación, y en este caso, más segura.
En los diferentes navegadores, podrás encontrar las extensiones recorriendo estos itinerarios:

- Firefox: ve a Herramientas ->Complementos ->Obtener extensiones.
- Chrome: ve a Herramientas ->Extensiones ->Obtener más extensiones.
- Internet Explorer: ve a Herramientas ->Administrar extensiones.
- Apple Safari: ve a Safari ->Extensiones de Safari.

Te recomendamos las siguientes extensiones:

- Poper Blocker (extensión de Chrome)
- Adblock Plus
- Better Pop Up Blocker
- Flashblock
- NoScript



Desde un programa específico

Aunque con las herramientas que te acabamos de proporcionar la protección está casi garantizada al 100%, hay gente que se toma muy en serio todo lo que a la seguridad se refiere, por eso, para los más exigentes, hay la opción de descargarse un programa específico y configurar las opciones a gusto del consumidor.

Algunos son gratuitos y otros hay que pagar por ellos. Éstos últimos te ofrecerán, además de las funcionalidades de todo lo anterior, alarmas, advertencias, servicio al cliente y extras de seguridad.

Los más populares son:

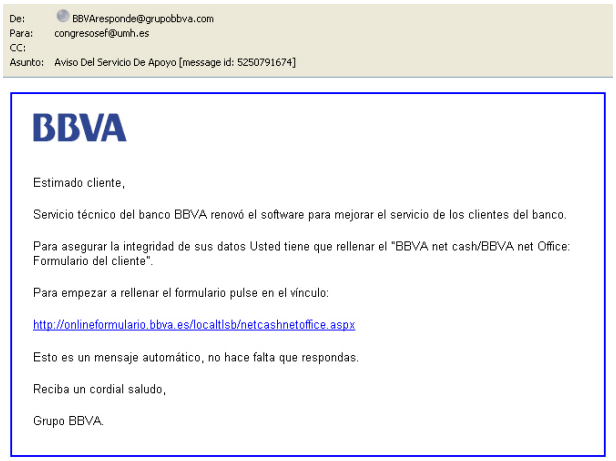
- Software gratuito:
    - AdFender
    - Smart Popup Blocker
    - Popup Free
    - Ad Arrest Popup Killer
- Software comprado:
    - Super Ad Blocker
    - Popup Ad Smasher
    - AdsGone Popup Killer
    - Popup Purger Pro

8. Fraudes más comunes en la red

1. **Phishing: Fraude en la banca online**

Qué es:

Se trata de un fraude de ingeniería social que consiste en sacar datos valorables de víctimas ingenuas. Los ataques de phishing más populares ocurren por mail. El cibercriminal crea un mensaje que parece fiable para el destinatario. El mail parece enviado por un banco importante que avisa al usuario de un probable accidente de seguridad: luego en el mensaje hay un enlace a través del cual el usuario puede proceder a la reconfiguración de la contraseña.El enlace en realidad lleva a una página web muy parecida a la del banco en cuestión. El usuario que ha seguido el enlace, se verá obligado a introducir su nombre de usuario y la contraseña para acceder a su cuenta y crear una nueva clave. En realidad, gracias a este truco, el cibercriminal está descubriendo las credenciales bancarias del usuario


De: BBVAresponde@grupobbva.com
Para: congresosef@umh.es
CC:
Asunto: Aviso Del Servicio De Apoyo [message id: 5250791674]

BBVA

Estimado cliente,

Servicio técnico del banco BBVA renovó el software para mejorar el servicio de los clientes del banco.

Para asegurar la integridad de sus datos Usted tiene que rellenar el "BBVA net cash/BBVA net Office: Formulario del cliente".

Para empezar a rellenar el formulario pulse en el vínculo:

http://onlineformulario.bbva.es/localtlsb/netcashnetoffice.aspx

Esto es un mensaje automático, no hace falta que respondas.

Reciba un cordial saludo,

Grupo BBVA.

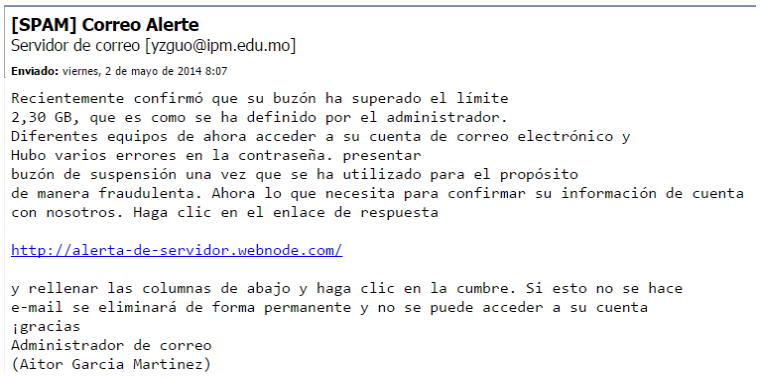
Cómo prevenirlo:

1. Nunca hacer clic en enlaces sospechosos
2. Reenviar el mail de phishing y el enlace a la compañía “imitada”;
3. En algunos casos, es necesario contactar con las fuerzas de policía;

4. También es buena idea informar a la entidad gubernamental de protección de los consumidores o empresas tecnológicas de referencia;
5. Al final de todo, borrar el mensaje.

Si ya te ha pasado:

- Actúa rápido
- Cambia las contraseñas por unas nuevas
- Notifica lo antes posible la incidencia a tu banco
- Denuncia el fraude a las Fuerzas de Seguridad del Estado: página web de la Guardia Civil para denunciar cualquier delito informático:



[SPAM] Correo Alerte
Servidor de correo [yzguo@ipm.edu.mo]
Enviado: viernes, 2 de mayo de 2014 8:07

Recientemente confirmó que su buzón ha superado el límite
2,30 GB, que es como se ha definido por el administrador.
Diferentes equipos de ahora acceder a su cuenta de correo electrónico y
Hubo varios errores en la contraseña. presentar
buzón de suspensión una vez que se ha utilizado para el propósito
de manera fraudulenta. Ahora lo que necesita para confirmar su información de cuenta
con nosotros. Haga clic en el enlace de respuesta

http://alerta-de-servidor.webnode.com/

y rellenar las columnas de abajo y haga clic en la cumbre. Si esto no se hace
e-mail se eliminará de forma permanente y no se puede acceder a su cuenta
¡gracias
Administrador de correo
(Aitor Garcia Martinez)

2. Fraude online: esperar algo que nunca llega

Qué es:

Es un tipo de fraude que consiste en ofertar en internet artículos con un precio muy inferior al valor real del producto, préstamos y ofertas de trabajo con condiciones muy atractivas. Cuando un comprador se pone en contacto con ellos, intentan cobrar por adelantado o forzar que el método de pago sea mediante MoneyGram, Western Union o plataformas similares y una vez la víctima ha enviado el dinero, el estafador desaparece.

- **Préstamos**

Podemos encontrar este tipo de anuncios en redes sociales, foros o mediante correos electrónicos. En todos los casos, nos ofrecen dinero con unas condiciones inmejorables: bajos tipos de interés y, por lo general, sin comprobación de la solvencia del solicitante. Cuando un usuario se interesa por estos préstamos, los ciberdelincuentes suelen buscar dos cosas de sus víctimas:

- **Dinero.** Normalmente, informan a la víctima que se le ha concedido el préstamo, pero le indican que debe adelantar una cantidad en concepto de gastos de gestión, un seguro de vida o cualquier otra excusa.
- **Información.** Al tratarse de un préstamo, se solicita a la víctima que envíe sus datos personales para tramitar la solicitud. Por ejemplo, una fotocopia del DNI, el número de la cuenta bancaria, el pasaporte y una foto reciente. Con todos estos datos, los estafadores pueden suplantar la identidad de la víctima.

- **Ofertas de empleo**

Los delincuentes conocen las necesidades de las personas que están desempleadas y las aprovechan para ofrecer trabajos falsos como gancho.
Existen dos casuísticas diferentes:
Fraudes consistentes en solicitar un adelanto económico al usuario:

- El anuncio de trabajo ofrece muy buenas condiciones de trabajo, exigiendo a cambio unos requisitos muy fáciles de acreditar por cualquiera.
- Una vez que el usuario contacta con el supuesto empleador manifestando su interés en el trabajo, puede realizar una pequeña entrevista telefónica o incluso no realizar ningún tipo de entrevista.

- El ciberdelincuente indica que estamos contratados y nos solicita una cantidad en concepto de adelanto para gestionar el alta en la seguridad social, para comprar la vestimenta laboral, gastos administrativos, etc.
- Cuando acudimos a la dirección indicada, nadie sabe del supuesto empleo.

Fraudes consistentes en captar muleros, personas que sin saberlo están participando en el blanqueo de capitales:

- El anuncio de trabajo nos ofrece un trabajo que consiste simplemente en recibir dinero mediante una transferencia y volver a enviarlo a otra cuenta bancaria. En el proceso, la víctima se queda con un porcentaje del dinero.
- El dinero que la víctima percibe en su cuenta procede de estafas y otras actividades delictivas, de tal manera que está colaborando con el crimen organizado y por tanto participando en la comisión de un delito.

Cómo prevenirlo:

Objetos baratos:

- Desconfía de las ofertas demasiado buenas.
- Evita las operaciones de pago que no dejen rastro y que soliciten el dinero por adelantado.
- No des datos personales.
- Busca información y valoraciones de otros usuarios.
- Revisa los datos legales de la empresa en la que se quiere realizar la compra

Préstamos:

En la mayoría de los casos se trata de préstamos ofrecidos a un interés muy bajo a personas con necesidad de financiación.

- Su manera de hacerse publicidad es a través de métodos poco convencionales, como por ejemplo mediante mensajes personales en redes sociales.
- Ofrecen el dinero a personas a las que las entidades bancarias tradicionales les han denegado el préstamo, aprovechando la desesperación. Debemos sospechar si alguien, sin ningún motivo aparente, nos ofrece dinero.
- La redacción de los correos parece estar hecha con algún sistema de traducción automática de Internet y utiliza expresiones que suenan extrañas en español.
- Piden dinero por adelantado antes de realizar cualquier operación.
- Hacer búsquedas en Google de algunas frases que contenga el mensaje nos puede ayudar a detectar un posible timo. A veces, tras una búsqueda, podemos encontrar a cientos de usuarios que han sido víctimas del mismo fraude.

Búsqueda de empleo:

Para detectar este tipo de engaños, debemos desconfiar de las ofertas de trabajo que cumplen los siguientes requisitos:

- Trabajo muy bien remunerado para un puesto sin cualificación.

- Se pide al supuesto empleado que abone una cantidad de dinero por anticipado.
- El envío de dinero se realiza normalmente a través de empresas como Western Union o MoneyGram.
- Las entrevistas de trabajo o no existen, o se realizan por teléfono o a través de Internet. No se realizan en las oficinas de la empresa.
- Usan cuentas de correo gratuitas como Gmail, Outlook, Yahoo, etc.

PUESTO DE TRABAJO – EDAD DE 20 A 50, SALARIO FIJO MAS PLUSES.

Empresa conocida televisivamente, precisa personal que cubra las siguientes expectativas:
PERSONAL AMBOS SEXOS.
DE 20 A 50 AÑOS.
FORMACION A NUESTRO CARGO.
IMPRESCINDIBLE:
Posibilidad 1) Llevar más de un año con el mismo banco o caja.
Posibilidad 2) Ser conocido/a en su oficina del banco o caja de confianza.
Posibilidad 3) Tener un conocido/a en su oficina del banco o caja de confianza.

SE OFRECE:
ALTA EN S.S.
FIJO DE 990 EUROS MENSUALES MÁS PLUSES.

Correo electrónico: **xxx** @hotmail.es
En el **ASUNTO** indica: **(POSIBILIDAD QUE CUMPLES, LA 1) LA 2) O LA 3)**
En el correo de respuesta recibirás detalles de la oferta, puestos, condiciones y entrevista.

- Los correos que envían son plantillas y apenas están personalizados.
- Las ofertas suelen llegar al correo sin que haya habido un proceso de selección previo.
- El trabajo ofertado suele ser a distancia, teletrabajo.
- Nos remiten algún fichero para que lo cumplimentemos con datos bancarios y personales.

Si ya te ha pasado:

Naturalmente depende de la situación, del vendedor y del método de pago utilizado. Pero, en general, para empezar se pueden hacer estas tres cosas:

1. Contacta con la organización de donde proceden los cargos en la tarjeta
2. Si no se soluciona el problema, contacta con el banco
3. En algunos casos, resulta necesario acudir a las autoridades policiales.

3. Pago online: que debes saber para realizar una compra segura

Comprar online en la actualidad es totalmente seguro. Sólo tenemos que tomar algunas precauciones y optar por la forma de pago más adecuada en cada caso:

- Busca tiendas online cuya dirección empiece por https y que muestren un candado en la barra de direcciones.
- Si tienes dudas sobre la fiabilidad de una tienda online, debes optar por plataformas de pago (por ejemplo PayPal) o pago contra reembolso.
- Si la tienda es conocida y fiable, puedes hacer el pago de forma segura mediante tarjeta de crédito, transferencia bancaria o tarjetas prepago.
- El uso de empresas de envío de dinero instantáneo no debe utilizarse para las compras por Internet, ya que no permite recuperar el dinero en caso de fraude. Estos envíos son seguros siempre que se envíe dinero a alguien de confianza

Con quién contactar en caso de cualquier fraude:
Unidad central de delitos telemáticos de la Guardia Civil:
https://www.gdt.guardiacivil.es/webgdt/pinformar.php
Formulario de la Policía Nacional para denunciar delitos online:
http://www.policia.es/formulario_generico.php?ordenes=52