

# EL EFECTO INTERNET

www.asi-mexico.org



*Querido @Santa:*

*¡Me urge que me traigas por favor!...*



## UNA GUÍA DE FACEBOOK PARA PADRES DE FAMILIA

No somos @Santa,  
¡Pero aquí te la traemos!



Año 1. Número 3.

Conoce la socialización digital



La radiografía del spam en México



# ALIANZA POR LA SEGURIDAD EN INTERNET A.C. – MÉXICO

## ¡DENUNCIE EL CONTENIDO ILEGAL O FRAUDULENTO EN INTERNET!

Usted puede ayudarnos a lograr que los usuarios de México utilicen Internet con toda tranquilidad

# Visítenos en [www.asi-mexico.org](http://www.asi-mexico.org)



**LÍNEA DE AYUDA PARA JÓVENES**  
Apoyo profesional por parte de la SPM en temas de uso compulsivo, ansiedad, impacto a conductas, etc.

**LÍNEA DE DENUNCIA**  
Reporte de contenido ilegal, inapropiado y fraudulento.

**BOLETÍN DE NOTICIAS**  
Mensual con información relevante sobre denuncias recibidas, nuevos sitios para menores, noticias sobre seguridad, resultados de encuestas, etc.

## CARTAS DEL LECTOR

### Amigos de El Efecto Internet:

**Y**o soy uno de los miles de usuarios que han recibido correos como los que describen en la sección "Internet S.O.S.", en el ejemplar número 2 de su revista. A mí me han dicho que fui beneficiario de una herencia en Somalia, que una persona falleció y dejó mucho dinero sin reclamar, y puedo ganar una parte sólo por ayudarlos a sacarlo de su país.

Es claro que éstas son sólo mentiras, pero lo que me interesa saber es de dónde sacan mi dirección de correo, o qué puedo hacer para que no me los sigan mandando.

Muchas gracias

*(Mensaje sin firmar)*

### Respuesta:

Ésa es una de las razones por las que titulamos el artículo "Las mil caras del Fraude Nigeriano", para indicar que son muchos los esquemas que los defraudadores utilizan, e incluimos ejemplos de los asuntos más comúnmente utilizados para engañar usuarios.

Existen muchas formas para obtener direcciones de usuarios y mandarles correos no solicitados. En este ejemplar vamos a iniciar la revisión de todo el escenario alrededor de esta calamidad digital, e incluiremos una explicación sobre cómo es que tu dirección puede caer en manos de malintencionados.

Tenemos evidencia de muchos

fraudes que se llegan a concretar y que se iniciaron por un correo electrónico, por lo que consideramos muy importante que los usuarios de todos los niveles conozcan esta problemática para que aprendan a autoprotgerse de ella.

### ¿Te gustaría colaborar?

Si tienes un artículo o contenido que pueda ser de utilidad para el usuario de Internet de México, piensas que puede ayudar a tener mejores experiencias con la red, y te interesa que lo publiquemos aquí, envíanos un correo a [editorial@asi-mexico.org](mailto:editorial@asi-mexico.org) y con mucho gusto lo consideramos.

**Envía tus comentarios, quejas y sugerencias a [contacto@asi-mexico.org](mailto:contacto@asi-mexico.org)**

[www.efectointernet.org](http://www.efectointernet.org)



# La socialización digital y el spam

La adopción masiva de los medios digitales como canal favorito de comunicación ha creado un nuevo orden social en el que, por ejemplo, por primera vez en la historia, una generación menor sabe más sobre un tema que las generaciones mayores. En otras palabras, los niños y adolescentes saben más sobre Internet que sus padres. Esto incluye, por supuesto, todos los medios digitales a su disposición como computadoras, celulares, videoconsolas y cámaras, con los que realizan la mayoría de sus actividades favoritas, como entretenerse y platicar con sus amigos.

En esta última frase reside la buena noticia para todos los padres de familia: sus hijos hacen casi lo mismo que ellos hacían cuando eran pequeños, sólo que lo realizan en forma masiva; ha cambiado el medio, pero no la actividad.

La gran mayoría de los jóvenes participan en las redes sociales en Internet, tecnología por demás fascinante que los mantiene en contacto con su grupo social. Es importante saber que unirse a una red social, como Facebook, no es lo mismo que socializar digitalmente; la mayoría de los niños encuestados en nuestro programa escolar manifiestan que sólo “subieron” su lista de amigos actuales, aquéllos con los que conviven diariamente por ejemplo en su escuela, pero no

han desarrollado nuevas amistades reales a partir de ahí. Además, las acciones tendientes a socializar se dan en varios medios, como blogs, mensajería y celulares, y no sólo en las redes sociales.

Para crear un perfil en una red social es necesario contar con una cuenta de correo electrónico, lo cual abre la puerta a recibir toda clase de mensajes no deseados, llamados *spam*, que es el vehículo favorito de los usuarios malintencionados para acercarnos intentos de engaño y fraude que impacten en nuestro patrimonio y, en ocasiones, en nuestra reputación. Es muy importante que platicues con tus hijos sobre esta calamidad digital.

Por ello en este ejemplar hemos dedicado la sección “Internet en tu familia” a explicarte ampliamente las redes sociales y el concepto de socialización digital, y presentamos la primera parte de la “Guía de Facebook para padres de familia” y la sección “Internet S.O.S.”, que habla de todo lo que necesitas saber sobre el *spam*, para que tú y tu familia puedan mantenerse apartados de riesgos y disfruten de todo el potencial de Internet tranquilamente.

**Comité Editorial,  
El Efecto Internet.  
www.efectointernet.org**

## ÍNDICE

<b>INTERNET EN TU FAMILIA</b>	<b>4</b>
¿Qué son las redes sociales?	5
Breve historia	7
Guía de Facebook para padres	10
<b>INTERNET S.O.S.</b>	<b>16</b>
La radiografía del <i>spam</i>	17
Prevención	23
Modus operandi	24
<b>EL ROL DE LA ESCUELA</b>	<b>26</b>
Internet sin riesgos	
Debate entre estudiantes	28

## DIRECTORIO

**DIRECTOR GENERAL**  
Armando Novoa Foglio

**DIRECTORA EDITORIAL**  
Rocío Moreno Rodríguez

**JEFE DE ARTE**  
Ramón Guerrero García

**CORRECCIÓN DE ESTILO**  
Joel Aguirre A.

**COLABORADORES**  
Lorena Velasco Moreno  
Martín Hernández Peña

(D.R.) Año 1, número 3. Editor responsable: Armando Novoa Foglio. Número Certificado de Reserva otorgado por Derechos de Autor: en trámite. Número de Certificado de Licitud de Título: en trámite. Número de Certificado de Licitud de Contenido: en trámite. Domicilio de la publicación: Grupo Editorial Via Satélite, S.A. de C.V. Progreso no. 42, col. Escandón, México, D.F. C.P. 11800. Tel. 52-72-60-88. Impresa en: Grupo Papel y Color S.A. de C.V. Avenida Tlamica, mz 13, lote 12, col. Bella Vista, Cuautitlán Izcalli, Estado de México. C.P. 54710. Distribución en locales cerrados: DIMSA, Mariano Escobedo no. 218, Col. Anáhuac. C.P. 11320, México, D.F. Tel. 52-62-94-00. Derechos reservados. Prohibida la reproducción total o parcial.

Los artículos y sus ideas expresadas son responsabilidad de los autores y no necesariamente reflejan la opinión de esta casa editorial.

**Información de Copyright ©**  
Todas las marcas y nombres comerciales utilizados en esta guía tienen Copyright de sus distintos titulares. Prohibida la reproducción total o parcial por cualquier medio. Todos los derechos reservados.



# Internet en tu familia

**Las redes sociales son el eje del nuevo paradigma de socialización digital, son extremadamente populares entre los niños y adolescentes de nuestro país, y todo un crucigrama para los padres de familia.**

**D**urante 2010, nuestra organización ofreció más de 40 conferencias escolares ante un aproximado de 10 000 padres de familia, con temas como “Privacidad en Internet”, “Seguridad activa para menores en Internet” y “Ciberciudadanía”, en las que se les presentan detalles de las actividades que sus hijos desarrollan en línea y que frecuentemente resultan ser en algún grado desconocidas para los adultos, cuando no totalmente ignoradas.



## ¿POR QUÉ NECESITAN SABERLO?

El misterio se convierte en preocupación cuando los incidentes negativos entre los menores de edad empiezan a ser cada vez más recurrentes. Ya nos resulta normal que en cada presentación que realizamos, al final se nos acercan uno o varios padres de familia que nos muestran copias de las demandas que han presentado por vías civiles o penales, porque a sus hijos los han humillado en portales falsos, difamado o incluso hasta amenazado, con el lamentable ingrediente adicional de que en casi todos los casos estas molestias provienen de otros menores de edad, casi siempre del mismo colegio, que en realidad lo hacen mayormente como travesura, pero que en ocasiones caen incluso en el supuesto de algún delito claramente tipificado en nuestra legislación.

Los medios digitales le han abierto las puertas a los niños y adolescentes, a la posibilidad de interactuar masiva y permanentemente con cientos y en ocasiones miles de personas, a una edad en la que no necesariamente tienen la madurez para desarrollar relaciones en forma sana, segura y responsable, por lo que necesitan la orientación de los padres de familia.

Para poder orientar a sus hijos eficientemente, los padres de familia necesitan la información que les permita entender sus actividades en línea y los riesgos a considerar, pero sobre todo, la mejor forma

de aprovechar la tecnología para su crecimiento personal. Por ello en esta sección te acercamos toda la información que como padre o madre de familia necesitas saber acerca del nuevo paradigma de la socialización digital, las redes sociales en Internet y su diferencia.

## SOCIALIZACIÓN DIGITAL

¿Qué debemos entender por socialización digital? ¿Es lo mismo que las redes sociales de Internet como Facebook, Hi5 y MySpace?

La respuesta corta es “no”, ya que socialización y red social no son lo mismo.

La socialización digital se define como la acción de “socializar en los medios digitales” disponibles en la actualidad, como Internet, celulares, consolas de videojuegos, cámaras digitales y, en general, cualquier dispositivo digital que nos permita entrar en contacto con otras personas.

## PERO, POR PRINCIPIO, ¿QUÉ ENTENDEMOS POR “SOCIALIZAR”?



Si bien la psicología nos provee diversas definiciones para el término, podemos partir de una definición funcional:

“Proceso por el cual el ser humano adquiere la experiencia de interrelacionarse con los demás, haciendo énfasis en el desarrollo de nuevas relaciones. Implica el gusto, la apertura y las acciones necesarias para conocer a otras personas, entendiendo y respetando los valores y las normas de conducta válidas en común para el grupo al que cada cual pertenece”.

En pocas palabras, al menos en el mundo real, en su interpretación más simple, podemos decir que socializar es la acción de salir y conocer nuevas personas.

#### NOTA:

Cabe aclarar que el término “mundo real” se utiliza aquí por la costumbre aceptada de aplicarlo cuando nos referimos al mundo físico y para distinguirlo del “mundo virtual”, término comúnmente aplicado a Internet y al conjunto de medios digitales que nos ofrecen acceso a la red. Sin embargo, hoy en día, y sobre todo cuando hablamos de las actividades de los jóvenes, es muy importante resaltar que todo lo que sucede en ese “mundo virtual” es absolutamente real, y puede impactar muy fácilmente en nuestra vida diaria. Un delito cometido en Internet se castiga en el “mundo real”.

Por supuesto que para socializar se requiere de ciertas habilidades que se desarrollan con el tiempo, como la autoexpresión, la comunicación interpersonal y la claridad, el valor, la comprensión, la interpretación del lenguaje corporal, la sensibilidad y muchas cosas más que nos ayudan a entablar relaciones con otros seres humanos.

Las generaciones anteriores socializábamos en el centro comercial, en fiestas o en el colegio. Las nuevas generaciones lo hacen en los medios digitales a su alcance, lo que establece de facto todo un nuevo orden social, o paradigma, pues las reglas, las normas e incluso las habilidades para hacerlo, han cambiado, aun cuando no se puede negar que las habilidades

tradicionales mencionadas en el párrafo anterior siguen siendo de gran utilidad en esta era.

## ENTONCES, ¿QUÉ SON LAS REDES SOCIALES?

Las redes sociales en Internet, como Facebook, Hi5 y MySpace, tan populares entre los jóvenes, son, en todo caso, un medio para socializar, pero sólo cuando el individuo desea aprovecharlas para ese fin, ya que ése no es el objetivo primario de estos servicios.

Veamos la definición que la prestigiada investigadora danah. m. boyd (ella prefiere escribir su nombre siempre en minúsculas) nos da en su papel de trabajo titulado “Social Network Sites: a definition”:

**Definimos como “Sitio de red social” a un servicio de Internet que le permite a un individuo:**

- 1. Construir un perfil público o semipúblico dentro de un sistema delimitado.**
- 2. Articular una lista de otros usuarios de la red social con los que mantenemos algún tipo de conexión.**
- 3. Ver la lista de conexiones de nuestros contactos, y cruzarla con la propia.**

Si nos atenemos a lo anterior, nos damos cuenta de que una red social no implica la acción de socializar, es sólo un medio para ello, pero sujeto a que ésa sea la intención que un usuario tenga al utilizar una red social.

En efecto, tener un perfil en una red social no implica per se que el usuario desee establecer nuevas relaciones con alguien, es más, se sabe que la mayoría de los contactos de un usuario son personas a las que conoce en el mundo real, si bien es indudable que ahí se proveen todas las herramientas que podamos imaginar para iniciar el proceso de socialización con miles de personas, lo que en ocasiones aparenta una convergencia entre servicios.

En todo caso, podemos citar otros servicios en donde evidentemente la intención participativa de todos los usuarios es únicamente la de conocer a otras personas, como son los sitios para hacer citas en línea, por ejemplo Match.com, cuya tecnología

permite poner en contacto a miembros del servicio con base en cotejar sus gustos y afinidades, para lograr relaciones duraderas, pues ése es su objetivo principal.

Veamos, como miembros de una red social en Internet, una vez que hemos podido ver la lista de los amigos de nuestros amigos, podemos presentarnos virtualmente con ellos haciéndoles llegar una petición para que nos acepten como amigos, felicitándolos el día de su cumpleaños, platicando de las personas y conexiones que tenemos en común, enviándoles regalos virtuales, que pueden ser tan simples como una taza de café, invitándolos a juegos y actividades dentro de la propia red social, y muchas cosas más, que han provocado que servicios como Facebook se conviertan en todo un fenómeno y sean increíblemente populares entre los usuarios de todas las edades, detonando ese nuevo orden social y redefiniendo a escala mundial conceptos como entretenimiento, comunicación, participación, sentido comunitario, democratización y participación social.

#### NOTA:

Establecidas las diferencias entre los términos “socialización digital” y “redes sociales”, es necesario aclarar que frecuentemente son utilizados en forma intercambiable, y presentados como sinónimos, lo que no deja de ser un error.

#### OTRAS FORMAS DE SOCIALIZACIÓN DIGITAL

Una buena forma de evidenciar la diferencia entre el concepto de socialización digital y redes Sociales en Internet es hacer énfasis en que el proceso de socialización se puede iniciar en otros medios digitales también, como son blogs (bitácoras digitales), foros, microrredes como Twitter, mensajería instantánea, grupos de noticias, y la participación en comunidades de intereses comunes, por ejemplo.

También las consolas de videojuegos nos ofrecen la tecnología para entrar en contacto con jugadores de otras latitudes, con los que podemos participar en una partida y posteriormente iniciar una amistad.

En todos esos medios podemos iniciar una nueva relación, por lo que debemos comprender que

#### LA SOCIALIZACIÓN DIGITAL ES UN CONCEPTO MUY AMPLIO QUE ABARCA VARIAS FACETAS DE LA COMUNICACIÓN DIGITAL ENTRE INDIVIDUOS.

Sin embargo, por su enorme popularidad y éxito, las redes sociales son el eje de este nuevo modelo de socialización. Es indudable que el simple hecho de descubrir que alguien que nos interesa es amigo o amiga de alguno de nuestros propios amigos, nos abre la puerta para tratar de acercarnos a esa persona, y es posible que esta feliz coincidencia sea algo que sin la tecnología de las redes sociales posiblemente nunca hubiéramos descubierto.

#### NOTA:

Los especialistas definen como “Conexión Latente” aquellas que existen entre dos personas que no se conocen, pero tienen algún amigo en común, y se acepta que la tecnología de redes sociales en Internet es un detonador para que estas relaciones se concreten.

#### FUNCIONALIDAD DE LAS REDES SOCIALES

¿Qué distingue a una red social de otra? ¿Por qué una es más popular que las demás?

Sin duda, las aplicaciones, funcionalidad y calidad de sus características, tanto en temas como entretenimiento y comunicación, como en aspectos más sensibles como la seguridad y la privacidad del usuario.

Independientemente de lo que las pueda diferenciar o hacer más atractivas, todas las redes sociales parten de la posibilidad de crear un perfil único para cada usuario. Al momento de unirse a una red social, una persona debe llenar un formulario con diversas preguntas o descripciones, como edad, sexo, estudios, localidad, etcétera, e incluso una descripción de quién es. Con todas estas respuestas se da de alta un perfil, al cual casi siempre se puede integrar una fotografía de la persona, lo que facilita su identificación. La información que cada usuario coloca en su perfil depende de su propia discreción.

Dependiendo de la red social a la que nos unimos, tendremos acceso a una serie de características de personalización diferentes, por ejemplo, para determinar la visibilidad del perfil, es decir, establecer

quién podrá verlo, si cualquier visitante, sólo nuestros amigos, los amigos de nuestros amigos, etcétera.

La gran mayoría de los conceptos que definen un perfil tienen valores por omisión, que hoy en día privilegian la seguridad y privacidad del usuario.

Algunas redes sociales permiten importar contactos desde otras aplicaciones, como mensajería instantánea, para verificar si ya cuentan con perfiles activos y anexarlos automáticamente a nuestra lista de amigos, aunque siempre hay que recordar que tal vez sean tan sólo conocidos que no deberían quedar calificados como amigos en realidad. La ventaja es que en todo momento se puede borrar a un amigo de la lista e impedir con ello que tenga acceso a ver nuestro perfil.

Es común en casi todas las redes sociales la posibilidad de dejar mensajes a nuestros amigos, con un método muy similar al correo electrónico, y esperar la respuesta posterior. Si un amigo está conectado al mismo tiempo que tú, es factible “conversar” con él en vivo, pues él o ella podrían responder tus mensajes tan pronto se los envíes.

**FACEBOOK**, la red social más popular a la fecha ([www.facebook.com](http://www.facebook.com)), permite instalar “aplicaciones”, que son elementos que extienden la funcionalidad de

tu perfil en todas direcciones; puedes elegir entre una gran cantidad de aplicaciones gratuitas para instalar juegos, enviar un café virtual, publicar la lista de tus amigos favoritos, crear encuestas sobre diferentes temas y una infinidad de componentes que ofrecen posibilidades ilimitadas de comunicación y entretenimiento, lo que sin duda cuenta para el enorme éxito de esta red social, tan ampliamente utilizada en nuestro país, y razón por la cual hemos publicado la guía de Facebook para padres de familia.

### UNA BREVE HISTORIA

En México, Facebook es por mucho la red social más utilizada. Si bien al inicio de 2008 aún era MySpace la favorita de los usuarios mexicanos, en ese mismo año Facebook tuvo un crecimiento espectacular que dejó muy atrás a sus dos principales rivales en todo el mundo: MySpace y Hi5.

El servicio Google Trends nos muestra gráficamente el cambio en las preferencias de los usuarios. Aquí se muestra en azul la penetración de Facebook en México, en café la de MySpace, y en naranja la de Hi5.

Según el blog Nearshore Americas, en julio de 2010 se estimaba que en México había 12.5 millones de usuarios, arriba de Argentina que contaba con 10 millones, y de Colombia con 9.7. En el caso de

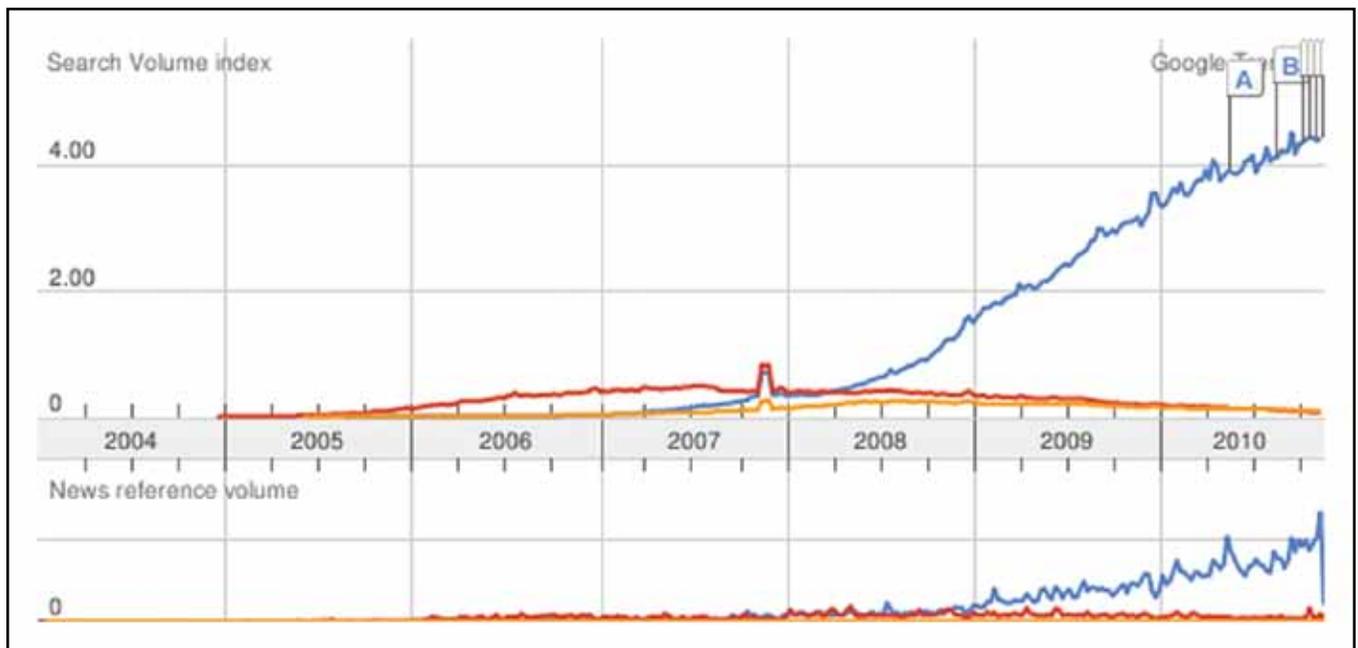


Fig. 1. La explosión de Facebook en México a partir de 2008.

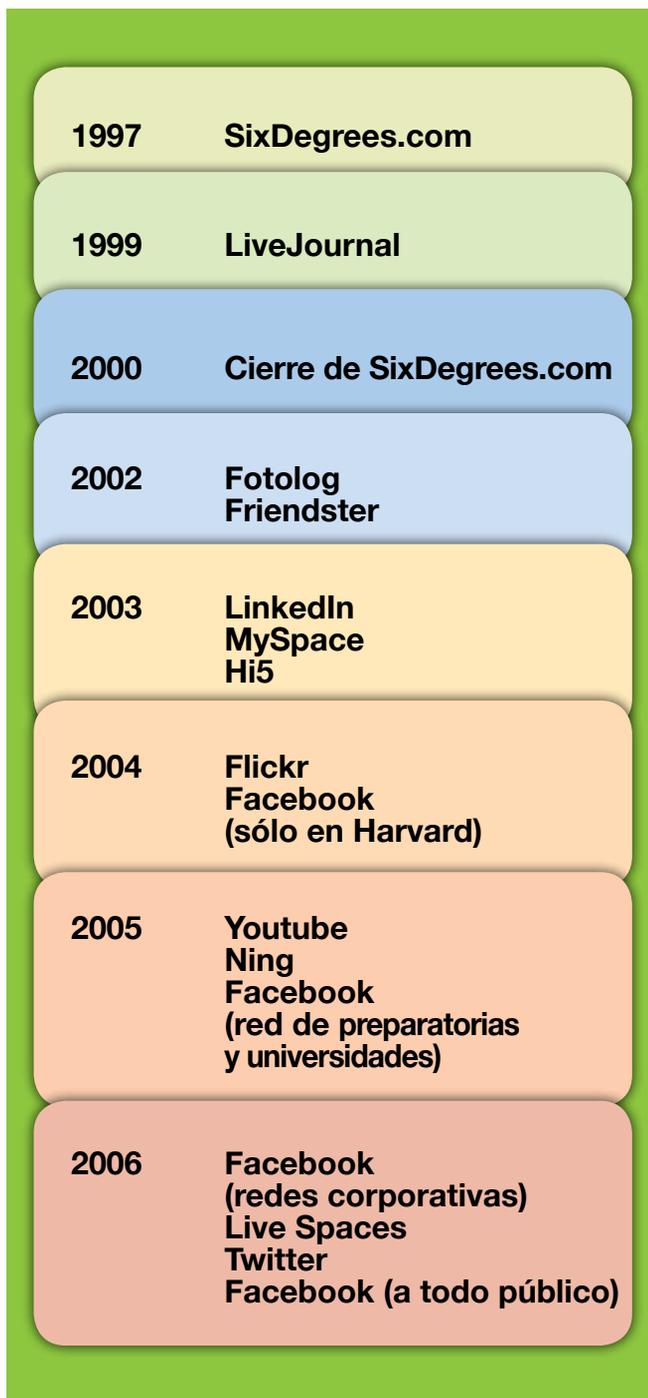


Fig. 2. Cronología de las redes sociales.

nuestro país, esto significa que más del 40% de los usuarios de Internet tienen un perfil de Facebook, y una gran mayoría de ellos utiliza también la igualmente popular microrred llamada Twitter, detonante de una transformación social que revisaremos en nuestro siguiente ejemplar.

Resulta sorprendente el crecimiento de las redes sociales en un lapso tan corto. La historia se remonta a 1997, cuando apareció la red llamada Sixdegrees.com. Si bien no todas las redes exitosas de los años siguientes iniciaron como tales, sí vivieron una rápida transformación para incorporar los servicios que podían atraer a un vasto número de usuarios. Resulta curioso que precisamente SixDegrees tuvo que cerrar en el año 2000, pues nunca pudo lograr un modelo financiero sustentable, y en palabras de su fundador, era un servicio que se adelantó a su época, sin lograr que los usuarios asimilaran el verdadero poder de esa tecnología.

Entre 1997 y 2001, varios portales ofrecieron servicios que combinaban la posibilidad de crear un perfil básico con las herramientas para enviar mensajes o localizar a contactos; algunos permitían manejar una especie de “diario digital”, popular entre el segmento femenino, todos ellos sin mayor éxito ni expansión.

En 2002, se lanzó el servicio llamado Friendster para competir con el portal de citas llamado Match.com, pero en lugar de tratar de establecer parejas entre desconocidos, intentaba crear relaciones entre amigos de amigos, asumiendo que habría una mejor posibilidad de que fueran exitosas al involucrar a los conocidos en común.

Varias fueron las razones por las que Friendster fracasó, algunas fallas técnicas hacían lentos sus servidores y la red atrajo a muchos “fakesters”, personas que creaban perfiles con información falsa, desilusionando a las posibles parejas y creando mala reputación a la red, lo que generó desconfianza que a la postre alejó incluso a los usuarios fundadores. Un dato curioso es que mientras este descenso ocurría en los Estados Unidos, la popularidad de la red social se detonaba en países como Filipinas.

Es precisamente por esto que en el siguiente ejemplar revisaremos el impacto global de las redes sociales, y la forma como han impulsado la colaboración internacional en temas como desastres naturales.

## FACEBOOK EN NÚMEROS

Como mencionamos antes, Facebook es por mucho la red social más popular en México, y a diferencia de otros países, aquí la población más grande de usuarios son menores de edad, cuyas actividades tienen perplejos a los padres de familia, que por fortuna han ido paulatinamente pasando de la preocupación a la ocupación, acercándose a esta poderosa tecnología para poder orientar a sus hijos más efectivamente, y descubriendo a su favor los innegables beneficios de las redes sociales, como localizar a compañeros de escuela a los que tenían sin ver más de veinte años, conectarse con familiares en todo el mundo, etcétera.

**PARA ELLOS HEMOS DADO INICIO A LA PUBLICACIÓN DE LA “GUÍA DE FACEBOOK PARA PADRES DE FAMILIA”,** que iremos entregando en los siguientes ejemplares y que estamos seguros será de gran utilidad. Si estás pensando animarte y crear tu propio perfil, te invitamos a revisar las recomendaciones de seguridad y reputación que publicaremos en el siguiente ejemplar.

El tamaño actual de Facebook es absolutamente impresionante. De su propia página de estadísticas se desprenden los siguientes parámetros:

### **Gente en Facebook:**

- **Más de 500 millones de usuarios activos.**
- **El 50% de los usuarios se conecta diariamente.**
- **El usuario promedio tiene 130 amigos en su perfil.**
- **La gente gasta 700 mil millones de minutos al mes dentro de Facebook.**

### **Facebook en el mundo**

- **Existen más de 70 traducciones del portal.**
- **Más de 300 000 usuarios cooperaron para traducir el sitio.**
- **Alrededor del 70% de los usuarios de Facebook se encuentra fuera de Estados Unidos.**

### **Actividad en Facebook**

- **Existen más de 900 millones de objetos con los que la gente puede interactuar, como páginas, grupos, eventos, etcétera.**
- **El usuario promedio se conecta a 80 páginas, grupos o eventos de comunidades.**
- **El usuario promedio coloca 90 piezas de contenido al mes.**
- **Más de 30 mil millones de piezas de contenido se comparten mensualmente (ligas, noticias, fotos, etcétera).**

## ¿Y QUÉ SUCEDE CON TWITTER?

Resulta absolutamente fascinante observar la interacción social que se desarrolla en esta llamada “microrred social”, en donde los usuarios crean cuentas que les permiten publicar mensajes (tweets) de un máximo de 140 caracteres, disponibles para la lectura de cualquier persona que visite la página del usuario, o bien, que se registre como “seguidor” del mismo.

**EN MUCHOS FOROS SE HA BAUTIZADO A TWITTER COMO EL “QUINTO PODER”,** ya que ha sido adoptado por un amplio segmento de usuarios del país como medio de “defensa social” contra medidas que se consideran de alguna forma impositivas y que por lo tanto son rechazadas por la sociedad.

Un muy claro ejemplo de lo anterior es el caso de los “alcoholímetros”, cuyas ubicaciones son localizadas y “twitteadas” para que todos los conductores los eviten, situación que ha creado una contrariedad a nivel autoridad, y ha desatado todo tipo de discusiones en foros y comunidades.

En el próximo ejemplar haremos una radiografía del origen de esta red, y las más populares aplicaciones que los usuarios mexicanos le están dando.

**Esperamos tus comentarios en  
contacto@asi-mexico.org**

**Comité editorial  
Alianza por la Seguridad en Internet**



# No somos Santa Claus, pero cumplimos tus deseos: aquí te presentamos la

# Guía de Facebook

# para padres de familia

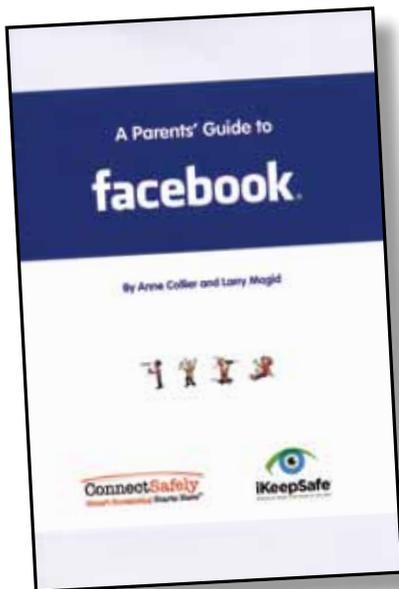
## Parte 1.

### Localización al español con autorización de ConnectSafely (c)

#### INTRODUCCIÓN

Bienvenidos a nuestra guía de Facebook para padres de familia! Ha sido diseñada para ayudarte a entender qué es Facebook y cómo poder usarlo en forma segura. Con esta guía podrás estar mejor informado y, por

ende, serás capaz de comunicarte con los usuarios jóvenes, entre ellos por supuesto tus hijos, de manera más efectiva. Esto es muy importante porque (1) si algo llega a salir mal, tu querías que tus hijos acudieran a ti, y (2) en la medida en que Internet se vuelve más social y móvil, la orientación parental y apoyo adquieren mayor relevancia para garantizar el bienestar de los menores ante los medios digitales y la tecnología con la que socializan.



de mercadotecnia, búsqueda de donativos y comunicación con clientes y asociados.

Es un hecho que Facebook no es la única red social, existen en realidad miles de ellas distribuidas por todo el mundo; algunas son redes sociales de intereses generales en algún país, y otras se refieren a intereses específicos en varios países, como deportes, cocina, apuestas, música, etcétera. Algunas redes sociales están diseñadas para poder acceder desde una computadora, y algunas son únicamente para teléfonos móviles. Facebook puede ser utilizada en ambos.

#### NOTA PARA LOS LECTORES

*Facebook agrega nuevas características, o bien actualiza algunas antiguas con cierta frecuencia. Esta guía ofrece la última información disponible al momento de su publicación original, en el otoño de 2010. Si encuentras algo en esta guía que consideres que no está vigente, por favor envíanos un mensaje a [contacto@asi-mexico.org](mailto:contacto@asi-mexico.org)*

#### ¿QUÉ ES FACEBOOK?

Facebook es una red social en Internet utilizada por más de 500 millones de personas en todos los países del mundo que abarca hasta ahora 70 lenguajes. La edad mínima para pertenecer a la red es de 13 años, pero los adolescentes representan sólo una minoría de la población que utiliza Facebook. El sitio es utilizado por una gran cantidad de adultos, muchos de ellos padres de familia. Pero no es utilizado sólo por individuos, también por empresas, organizaciones y hasta gobiernos en todo el mundo para labores

#### ¿QUÉ HACE LA GENTE EN FACEBOOK?

Platicar, compartir fotos ( más de 100 millones de fotos nuevas cada día!), subir videos, mantenerse en contacto y compartir noticias personales, jugar, planear juntas y reuniones familiares o de amigos, enviar felicitaciones en cumpleaños y festividades, hacer la tarea o negocios con otras personas, encontrar amigos de la infancia, revisar opiniones sobre libros, recomendar restaurantes, apoyar causas sociales y un muy largo etcétera.

En realidad es muy poco lo que una persona no podría hacer en Facebook. A veces llamada “utilería social”, se asemeja a una planta de energía que provee la plataforma para las actividades diarias pero siempre dinámicas de todos sus usuarios, 24 horas al día, siete días a la semana. La cantidad de actividad en Facebook es casi inconcebible. Cada mes, los propios usuarios colocan 30 000 millones de piezas de contenido en esta red, como son comentarios, fotos, videos, etcétera.

En efecto, el “producto” llamado Facebook es algo vivo que cambia constantemente y es generado por los propios usuarios. A diferencia de los medios con los que las generaciones mayores crecimos —libros, periódicos e incluso radio y televisión—, podemos verlo como el producto colectivo de las vidas diarias de millones de usuarios (no sólo sus relaciones sociales, pero todo lo que hacen), que se actualiza en forma espontánea, en todo momento, alrededor de todo el mundo. Es un gran espejo que refleja los pormenores del quehacer humano dentro y fuera de Internet.

## ¿POR QUÉ LOS JÓVENES USAN FACEBOOK?

Por las mismas razones que lo hacen los adultos. Las investigaciones de psicólogos y sociólogos nos enseñan que los menores utilizan las redes sociales en Internet para:

- Socializar o “salir” con sus amigos, que en su mayor parte son de su propia escuela.
- Mantenerse al día sobre lo que hacen amigos, relaciones, parientes, y de lo que sucede en los grupos a los que pertenecen.
- Colaborar en trabajos escolares.
- Más de 30 mil millones de piezas de contenido se comparten mensualmente (ligas, noticias, fotos, etcétera).
- Buscar apoyo emocional o validación.
- Desarrollar su autoexpresión y exploración de identidad, aspectos tradicionales del desarrollo adolescente.
- Lo que los sociólogos llaman “aprendizaje informal”, ese que sucede fuera de la estructura formal de la escuela. Esto incluye normas sociales y adaptación social.



- Aprender habilidades técnicas para su desarrollo en esta era digital.
- Descubrir y explorar intereses, tanto académicos como para un futuro laboral.
- Aprender sobre el mundo que está más allá de su casa y escuela, es decir, de su propio entorno.
- Participación ciudadana, en causas que pueden ser significativas para ellos.

## ¿FACEBOOK ES SEGURO?

Al igual que el mundo real, ninguna red social, sitios de citas en línea, de realidad virtual, juegos o cualquier otra forma de socialización digital, puede ofrecer una garantía de seguridad al cien por ciento, y por supuesto esto incluye a Facebook.

## ¿POR QUÉ?

Porque estamos hablando del Internet social, y la seguridad depende en gran parte de las conductas que una persona desarrolla hacia los demás. Facebook ofrece características de seguridad y privacidad, así como educación para sus usuarios. Los padres de familia se pueden beneficiar si visitan el centro de seguridad de Facebook (actualmente en [www.facebook.com/safety](http://www.facebook.com/safety)), un recurso de fácil comprensión con información para menores, padres de familia, educadores y agencias de investigación.

Este centro, así como esta guía, son importantes por la simple razón de que el “producto” Facebook es creado precisamente por la comunidad. Los padres de familia necesitan saber que en el Internet social la seguridad es una responsabilidad compartida, una constante negociación entre los propios usuarios (por

ejemplo, para colocar una foto en que aparecen varios de ellos), entre usuarios y el propio sitio, y entre los usuarios menores y sus padres.

Así que la respuesta corta a la pregunta de si Facebook es seguro, en este entorno de masiva socialización digital, es que la seguridad depende tanto del usuario como del propio sitio. Por ello los padres de familia necesitan estar bien informados y mantener bien abiertas las líneas de comunicación con sus hijos, porque los jóvenes, como todos los usuarios de Facebook, están en permanente comunicación y comparten contenidos todo el tiempo.

### ¿CUÁLES SON LOS RIESGOS QUE IMPLICA LA SOCIALIZACIÓN DIGITAL?

La investigación de riesgos asociados con las actividades en línea de los menores de edad ofrece cinco importantes conclusiones:

1. Los jóvenes que se comportan de manera agresiva en línea tienen el doble de posibilidades de convertirse en víctimas a su vez, por lo que el comportamiento de los niños es clave para su propio bienestar en las redes sociales.
2. El riesgo más común que puede enfrentar un menor de edad es el hostigamiento por parte de sus conocidos, lo que incluye conductas dañinas, agresivas y difamatorias.

3. El entorno psicosocial de un menor, como su casa o escuela, es más propenso para implicar riesgos que la tecnología que utiliza.
4. No todos los menores están expuestos a los mismos riesgos, y los que son más propensos son precisamente los que también son proclives al riesgo en el mundo real.
5. Si bien para la gran mayoría de los menores de edad, su red social es un fiel reflejo de su vida real, también puede ser un medio para ampliar, masificar y hacer perpetuos sus conflictos y problemas. Cualquier cosa que se dice o publica cuando están enojados o por impulsividad, es muy difícil de retirar o retractarse, por lo que hoy más que nunca es muy importante (para todos los usuarios, incluso adultos) pensar antes de “hablar” en una red social, es decir, antes de publicar un comentario, enviar un mensaje o subir un video.



Algunos riesgos específicos de las redes sociales para los menores de edad incluyen:

- Publicar información sobre ellos mismos que a) pueda ayudar a un extraño a conocer su ubicación física, b) pueda ser usada para manipular o chantajear al usuario, o c) ya sea que la publique el mismo usuario u otra persona, pueda causarle daño emocional o poner en riesgo su reputación.
- Acoso u hostigamiento en línea (llamado *cyberbullying*).
- Estar demasiado tiempo en línea, perdiendo el equilibrio con otras actividades (“demasiado” es un término subjetivo, otro punto por el cual los padres deben involucrarse).
- Exposición a contenido inapropiado (aún más subjetivo), si bien es sabido que mucho peor contenido puede ser encontrado en otras partes de Internet, fuera de redes sociales con políticas responsables, como Facebook.



- Contacto potencial con adultos. Los padres deben estar pendientes de que la socialización digital de sus hijos no derive en encuentros no autorizados.
- Daños a su reputación y posibilidades de acceso a oportunidades en el futuro, ocasionadas por contenido publicado en momentos de enojo o alteración, ya sea por ellos mismos o por sus conocidos.

## COMO PADRES, ¿CÓMO PODEMOS ORIENTAR A NUESTROS HIJOS EN FACEBOOK?

Al igual que en la vida diaria de tus hijos, tu participación es clave para ayudarlos a formar una identidad positiva, mantener buenas relaciones y tener una buena reputación en el Internet social. Aunque más adelante daremos recomendaciones específicas, aquí te damos algunas ideas básicas de “parentalidad digital” que conviene tener presentes:

**Facebook es extremadamente personal.** Ésta es la razón por la cual la mejor recomendación es “platicar con tus hijos”. No creas todo lo que lees o escuches acerca de Facebook, sobre todo lo que proviene de los medios tradicionales de comunicación, que con frecuencia ofrecen una imagen negativa. Los adultos que no comprenden el concepto del Internet social o de la socialización en medios digitales, en ocasiones confunden el uso de Facebook como una actividad que puede provocar “adicción” en los jóvenes. En todo caso, a los que serían adictos es a sus propios amigos o a la experiencia de socializar.

Incluso dos menores de la misma familia pueden usar Facebook de manera muy diferente. Un estudio reciente descubrió que 1) incluso entre los usuarios más activos, Facebook no ha logrado remplazar



sus intereses en el mundo real, como deportes o música, y 2) aun cuando puedes mantener siempre abierta la conexión a Facebook, ésta permanece en segundo plano mientras realizan otras actividades. Cabe resaltar que los padres deberían involucrarse para determinar si hay un decremento en el rendimiento académico cuando los menores realizan las tareas escolares con la conexión a Facebook abierta, ya que evidentemente implica una potencial distracción.

**Como padre o madre, eres parte de la solución.** Tus hijos necesitan tu respaldo cuando algún incidente negativo sucede. Por esta razón, necesitas conocer todas sus actividades en línea y no sólo las que realizan en Facebook.

**Si algo negativo sucede, no sobre-reacciones.** Es otra situación en la que sirve mucho estar bien informado. Un padre (o madre) informado es un padre tranquilo, y es más fácil que un hijo acuda a sus padres cuando sabe que la conversación se llevará a cabo en forma tranquila y reflexiva. Como padres de familia debemos saber que podemos ayudar mucho a nuestros hijos si ellos tienen la apertura de venir a platicarnos sus problemas, por lo que debemos mantenernos siempre abiertos a esta posibilidad.

**Las herramientas de parentalidad digital.** Incluyen el refuerzo de los valores familiares tradicionales (honestidad, respeto, etcétera), el establecimiento de normas y límites claros y firmes (como por ejemplo, el horario en que los dispositivos digitales pueden ser usados) y, en ocasiones, el uso de la tecnología misma, como es el caso de los programas de control parental y filtrado



de contenido. Si tus hijos no son precisamente comunicativos acerca de sus actividades en línea, puede ser conveniente instalar un programa de este tipo para saber, por ejemplo, los sitios que visitan. En estos casos es muy recomendable hacerles saber que instalarás ese programa para que ellos no se sorprendan cuando descubran que tú estás enterado de sus visitas, y las pláticas al respecto no se conviertan en discusiones.

### **Facebook puede ser una excelente herramienta de parentalidad.**

Te puede brindar una curiosa ventana hacia la vida social de tus hijos y ayudarte a mantenerte informado sobre sus actividades. De hecho, es una buena idea que le preguntes a tus hijos cómo manejan los parámetros de seguridad y privacidad de esta red social. No sólo aprenderás sobre Facebook, también sabrás si ellos lo utilizan inteligentemente. Si hasta ahora no habías pensado en los parámetros de privacidad, podrás apoyarte en los que presentaremos en esta guía más adelante para que los revises con tus hijos. Además, considera la conveniencia de crear tu propio perfil en Facebook para que puedas ser un “amigo” de tus hijos en la red, muchos padres de familia hacen esto en todo el mundo, y la aprovechan como herramienta de parentalidad moderna. Si haces esto, ten mucho cuidado al escribir en su muro o dejar comentarios sobre lo que publican, pues los puedes avergonzar ante sus amigos, lo que con seguridad provocará una barrera de comunicación con ellos. Si tienes algo que comentarles sobre el contenido de sus perfiles, hazlo en forma directa en el ámbito familiar.

### **FORMAS DE MONITOREAR LAS ACTIVIDADES DE TUS HIJOS EN FACEBOOK**

Como se mencionó previamente, la mejor forma consiste en tener tu propio perfil y ser aceptado como “amigo” por tus hijos. Puede ser conveniente



establecer una regla familiar que señale que “ningún miembro de la familia puede bloquear a otro” sobre el contenido que publican en Facebook. Los padres de familia deben resistir la tentación de hacer comentarios en las páginas de sus hijos, recuerda que los miembros de la familia siempre pueden enviarse mensajes privados entre ellos, tal como se hace con el correo electrónico.

Algunos jóvenes pueden estar dispuestos a tener a sus padres como amigos en su perfil, pero pueden sentir pena de que sus nombres aparezcan en su lista de amigos. Algunos padres de familia resuelven esto creando un perfil con un nombre diferente, aun cuando esto no está permitido en el reglamento de uso de Facebook. Otro recurso al que los padres de familia recurren, es a tener acceso a las contraseñas de sus hijos, lo cual puede funcionar sobre todo con los más pequeños, ya que se ha visto que los adolescentes se oponen a darle a sus padres semejante nivel o capacidad de monitoreo, y prefieren utilizar otros sitios en forma secreta para las actividades que consideran privadas. El nivel de privacidad de un menor depende mucho de su forma de ser y de su propia relación con su familia, así como de los valores y reglas de ésta.

También puede ser de ayuda escribir el nombre completo de tus hijos, su dirección o número de teléfono en un buscador como Google, para enterarte de si hay cosas que se digan sobre ellos en cualquier parte de Internet.

Hay servicios de paga que monitorean la reputación en línea de las personas, como SafetyWeb y SocialShield, a los que te podría convenir suscribirte si sus servicios abarcan el país en el que vives. De esa forma puedes conocer lo que publican tus hijos en línea sin tener que crear tu perfil en Facebook y que te acepten como amigo.

En el siguiente ejemplar hablaremos de seguridad, privacidad y reputación en la era digital, huellas digitales y buena reputación, y revisaremos la optimización de parámetros de seguridad y privacidad de Facebook para menores de edad.

**Esperamos tus comentarios en  
[contacto@asi-mexico.org](mailto:contacto@asi-mexico.org)**

facebook

# Protege a tus hijos de los peligros de Internet

**H**oy en día las habilidades que nuestros hijos han desarrollado en el manejo de la tecnología para muchos de nosotros supera las expectativas. Desde temprana edad, entran en contacto con todo tipo de herramientas tecnológicas que los retan a descubrir nuevas formas de aprender, divertirse y conocer el mundo que los rodea.

Particularmente, el uso de Internet es cada vez más común entre los distintos segmentos de la sociedad. La facilidad con la que un niño o adolescente puede acceder a todo tipo de información nos preocupa y nos ocupa como padres de familia.

Internet se ha convertido en la herramienta en la que nuestros hijos prácticamente encuentran toda la información que buscan: definiciones, historias, biografías, mapas, estadísticas, deportes, cine, música, juegos... La lista es inmensa.

Ahora, con el auge de redes sociales como Facebook, Twitter y Youtube, nuestros hijos pueden pasar horas frente a una computadora sin darse cuenta y compartir información personal o familiar sin dimensionar las consecuencias que pudiera haber si llegara a manos de alguna persona malintencionada.

Por otro lado, en este mundo virtual existen millones de páginas con contenidos para todas las edades.

Internet no hace distinciones y muestra todo tipo de resultados cuando generamos una búsqueda, por lo que no es recomendable dejar a nuestros hijos sin supervisión, pero al mismo tiempo no podemos evitar que las utilicen, son parte de nuestra realidad.

Sabemos que no es fácil identificar qué están haciendo nuestros hijos, sin embargo, la tecnología también ha avanzado en el desarrollo de herramientas que permiten monitorear y controlar la relación de Internet con nuestros hijos.

Una de las herramientas más innovadoras del mercado es True@ Home, una tecnología sencilla que permite ver desde donde estés y en tiempo real todo lo que hacen tus hijos en la computadora: ¿con quién chatean?, ¿qué páginas visitan?, ¿cuánto tiempo dedican a sus tareas?, ¿sobre qué temas se interesan? El programa te muestra con qué personas interactúan y por cuánto tiempo; puedes comprobar si son o no personas conocidas y se activan alertas donde se resaltan las actividades que pueden ser inapropiadas para tus hijos. En resumen, permite monitorear todo lo que sucede mientras tu hijo está en la computadora y de esta forma planear con ellos las reglas del juego.

El gran reto que tenemos como padres es protegerlos sin limitar su libertad ni truncar su curiosidad y aprendizaje.

Protege a tus hijos de los peligros de Internet con  True@Home

Identifica de forma sencilla:

- Que páginas están visitando
- Con quién chatean
- El tiempo que pasan en la computadora



Te recomendamos utilizarlo en la computadora de escritorio **HP S5500LA**

SKU VT697AA#ABM Monitor A Elegir (w1858) Procesador Intel® Pentium® E5400 Memoria 2GB DDR3 Disco Duro 500GB Óptico SuperMulti DVD Burner with LightScribe Technology Sistema Operativo Windows® 7 Home Basic 64-bit

CompuSoluciones



Contáctanos:

Guadalajara, México y Monterrey 5000 7777

[mercadotecnia@compusoluciones.com](mailto:mercadotecnia@compusoluciones.com)

[www.compusoluciones.com](http://www.compusoluciones.com)



# Internet S.O.S.

¿Quién te puede ayudar si eres víctima de un delito en Internet?  
Con la colaboración especial de la Unidad de Investigación Cibernética (UIC)  
de la Procuraduría General de Justicia del Distrito Federal (PGJDF)

## La radiografía del *spam* en México

La importancia de Internet como medio de comunicación crece cada día, y al igual que en el resto del mundo, el correo electrónico es el canal más utilizado por los usuarios mexicanos para el envío de mensajes de todo tipo. Según la Asociación Mexicana de Internet, en el país tenemos 30.6 millones de usuarios, de los cuales, el 75% utiliza el correo electrónico.

Debido a lo anterior, es fácil entender que los usuarios malintencionados e incluso delincuentes cibernéticos, también se aprovechan del correo electrónico para orquestar todo tipo de intentos de fraude y buscar víctimas potenciales.

En el ejemplar anterior presentamos un caso real del llamado “Fraude Nigeriano”, recibido en nuestra Línea de Denuncia, que demuestra la facilidad con la que podemos caer en estos engaños y ver afectado nuestro patrimonio cuando hacemos caso a “propuestas” o contactos que recibimos por medio del correo electrónico. Ese artículo provocó que receptáramos una gran cantidad de comentarios de lectores que han recibido correos similares y que solicitan más información sobre el tema para aprender a protegerse.

Es obvio pensar que si recibimos un correo que intenta engañarnos para cometernos un fraude, nosotros no lo habríamos solicitado. El correo no solicitado, o *spam*, también llamado “correo basura”, es una auténtica calamidad digital que causa estragos de todo tipo a nivel mundial, y por ello es combatido en varios frentes, como son la legislación, la autorregulación de los proveedores de acceso a Internet (ISP), las políticas corporativas, etcétera.

Sin embargo, cuando nos damos cuenta de que tan sólo en el sistema Prodigy se eliminan más de 91 millones de correos en promedio diariamente por tratarse de *spam* (año 1, núm. 2), resulta evidente que los usuarios de todos los niveles debemos entender esta calamidad, y aprender a autoprotegernos de ella. En esta sección te presentamos todo lo que necesitas saber para evitar caer en engaños y seguir manteniendo esta importante tecnología siempre a tu favor.

### EN ESTE EJEMPLAR VAMOS A REVISAR:

1

#### La radiografía del *spam*

Origen, tipos de *spam* y cómo te puede afectar.

2

#### Recomendaciones de prevención

Ideas prácticas para alejarte del correo no solicitado.

3

#### Modus operandi

Un ejemplo real aportado por la UIC de la PGJDF para que conozcas la forma en que te puede afectar.

Y para darte un panorama completo alrededor de esta problemática y estés mejor preparado para combatirla, en el siguiente ejemplar te explicaremos:



## 1. ¿Por qué te llegan correos no solicitados?

## 2. ¿Es delito el *spam* en México?

**Recuerda:** si recibes un correo no solicitado que intenta cometer un fraude en tu contra, o consideras que presenta contenido ilegal, no dejes de denunciarlo en [www.asi-mexico.org/denuncia](http://www.asi-mexico.org/denuncia)

1

### LA RADIOGRAFÍA DEL SPAM

#### Origen del término *spam*

Es curioso que, originalmente, el término *spam* no tenía nada que ver con el correo electrónico. En 1937, la empresa Hornel Foods lanzó una carne enlatada llamada Hornel's Spiced Ham. El gran éxito de este producto se basó en que la lata incluía un mecanismo de apertura que libraba al consumidor de la necesidad de usar un abrelatas y no requería refrigeración. Su popularidad logró que el nombre se volviera genérico, y así como hoy en día a cualquier pañuelo desechable le llamamos "Kleenex", *spam* es el acrónimo de Spiced Ham.

Más adelante el grupo británico Monty Phytton hizo burla del producto que ya se encontraba en todas partes. En un sketch cómico presentó a un grupo de vikingos tratando de comer en una taberna, cuya propietaria les recitaba el menú, que incluía huevos con *spam*, tocino con *spam*, salchichas con *spam*, *spam* con *spam*, *spam*, *spam*, *spam*. Al final los vikingos cantan alegremente repitiendo el término a coro.

Alrededor de 1970, el término *spam* ya se usaba en Inglaterra y en EU para referirse a cualquier cosa que fuera abundante. Por esas fechas el consumidor se empezó a cansar del producto, e incluso hubo campañas para desprestigiarlo, ya que teóricamente era malo para la salud, con lo que el término *spam* se empezó a aplicar a cosas abundantes y no deseadas, lo que explica muy bien por qué le queda perfectamente al molesto correo no solicitado.

#### TIPOS DE SPAM

Hemos recibido reportes de *spam* en:

- a) Correo electrónico.
- b) Mensajería instantánea (también llamado *spim*).
- c) Foros.
- d) Blogs.
- e) Teléfonos móviles.
- f) Grupos de noticias.

Sin embargo, por su abundancia y mayor potencial de impacto negativo, nos referiremos al *spam* en correo electrónico, aunque, como se verá, muchos de los conceptos, sobre todo de prevención, aplican en cualquier plataforma.

#### Temas de *spam* en el correo electrónico

En cualquier caso estamos hablando de correos que nos ofrecen información que puede o no interesarnos, pero que nosotros no solicitamos!

Si bien hay ocasiones en que el correo contiene simple información comercial de productos o servicios y sólo son una molestia constante que satura nuestro buzón de entrada (como es el caso de las molestas cadenas), en la mayoría de los casos incluye tecnología que puede desde modificar nuestro navegador para que siempre abra una página comercial, hasta causar daño al equipo, información o al patrimonio del usuario, por lo que es importante la precaución.





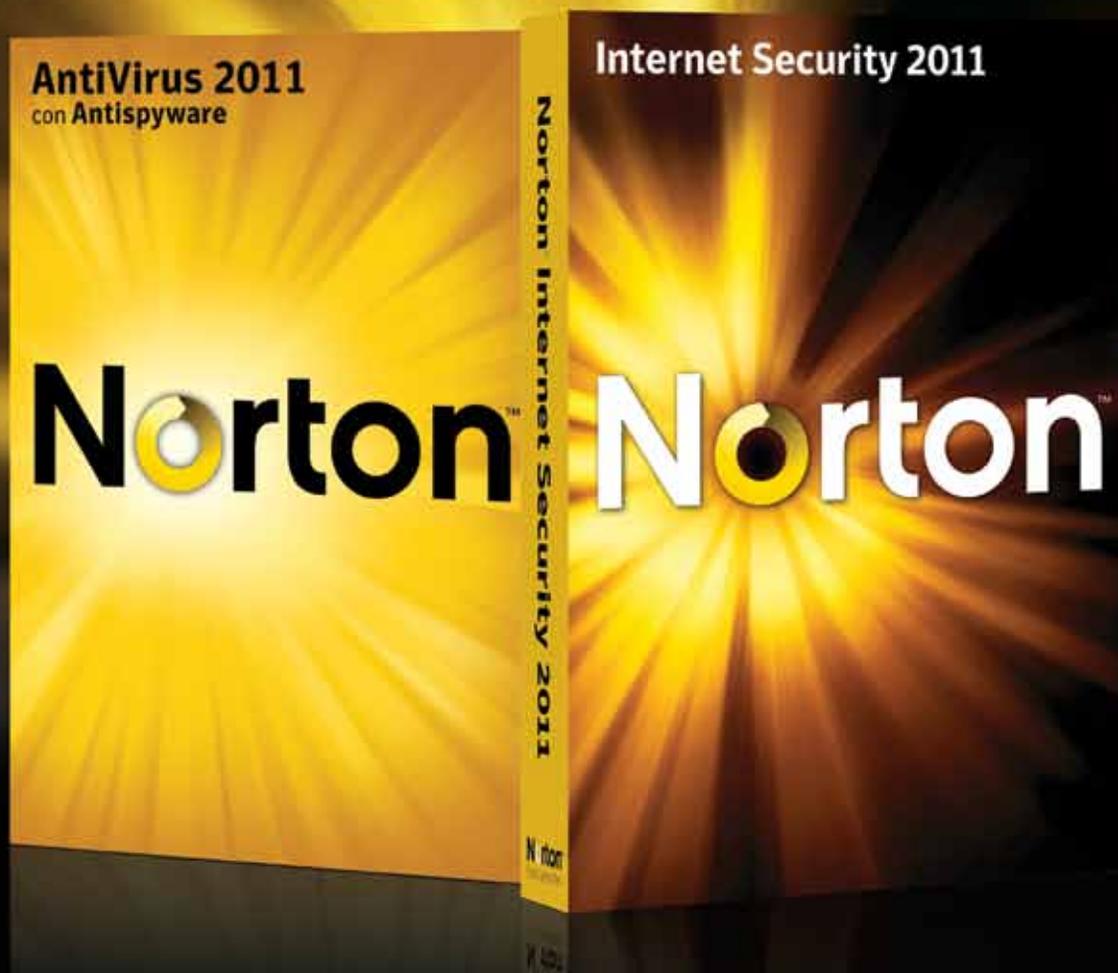
A nivel mundial, los temas más recurrentes en el spam son los siguientes.

- Pornografía
  - “ Compré una webcam y quiero que me veas desnuda!”.
  - “Satisface a tu pareja”.
- Salud
  - “ Baja de peso en una semana!”.
  - “Compra Valium a precio de mayoreo”.
- Piratería
  - “Ofrecemos licencias OEM al 10% de su valor”.
  - “No pagues precios de lista, tenemos grandes ofertas en marcas comerciales”.
- Educación
  - “Consigue tu diploma universitario”.
  - “Gradúate desde tu casa, precios accesibles”.

En México, los temas más comúnmente reportados en la Línea de Denuncia de ASI son:

- Cadenas
  - Te piden que le avises a todos tus contactos sobre nuevos virus, oraciones por la paz, etcétera.
- Fraude Nigeriano
  - Te escribe un supuesto funcionario bancario corrupto de algún país lejano (normalmente africano o del Este de Europa) que busca sacar grandes cantidades de dinero con tu ayuda ofreciéndote una jugosa comisión. Pueden hacerte creer que ganaste una lotería, eres el beneficiario de una herencia, te han otorgado un crédito, etcétera. Éste es uno de los temas de engaño con más reportes.
  - También llamado opt-out, todo newsletter debe ofrecer al usuario un mecanismo para dejar de recibir los correos. Si no lo tiene, o bien, si pides la cancelación y no te hacen caso, debes reportarlo en Profeco.
- Ofertas de pornografía gratuita
- Ofertas falsas de trabajo
  - Personas que enviaron sus datos completos y curriculum en una solicitud de trabajo, pero son contactados por alguien externo quien les ofrece asignarles el puesto a cambio de dinero.
- Phishing bancario
  - El usuario recibe un mensaje supuestamente desde su banco en que se le informa que por diferentes razones es necesario que actualice sus datos completos, y ofrecen ligas que te llevan a portales igualmente falsos que intentan robar tu información confidencial.
- Tarjetas postales falsas
  - Clásico mensaje que dice “Un amigo te ha enviado una postal”, ahora usan nombres comunes para tratar de engañarte, por ejemplo, “Manuel te ha enviado una postal”, buscando la posibilidad de que conozcas a alguien que se llame Manuel.
- Recargas de tiempo aire
  - Sin duda, es el tema más frecuente con el que se busca engañar al usuario ofreciendo el doble o triple de tiempo aire siguiendo ligas o instrucciones falsas.

# Norton™ hace mucho más



Anticípese a las amenazas para su equipo con la protección más rápida del sector. Norton AntiVirus 2011 detecta y elimina virus y otros peligros para permitirle conversar, enviar correo electrónico y compartir archivos de manera segura.

Navegue en Internet y haga compras y operaciones bancarias en línea de manera segura con Norton Internet Security 2011 la protección más rápida y ligera del sector.

## Cada click importa.

Protección rápida y ligera contra las amenazas para la seguridad del equipo.

**Norton™**  
from symantec

- Robo de contraseñas

Muy difundido entre los jóvenes, son mensajes que te ofrecen darte a conocer quién te ha borrado de su mensajería instantánea, pero te piden tu nombre de usuario y contraseña y comúnmente la conservan para mandar mensajes en tu nombre a terceros.

- Diversos

“Es la última vez que te molesto”. “¿Ya te olvidaste de mí?”. Son mensajes que llegan como si vinieran de tu misma cuenta de correo: piratería, invitaciones a cursos, servicios de asesorías, etcétera.



Los delincuentes no hacen uso de complicados mecanismos o tecnología para obtener tu información o patrimonio, pero logran engañarte para que tú mismo lo entregues. El ejemplo más ilustrativo es el de la oferta de duplicar tu tiempo aire enviando un código por SMS al 7373 después de abonar una tarjeta de 100 pesos.

Te llega un correo electrónico que te invita a abonar una ficha de 100 pesos a tu línea de celular, y una vez que lo hayas hecho, mandes un mensaje con una clave (que el correo te señala) al número 7373:

La verdad es que así es como se transfiere saldo de un celular a otro en el sistema de Telcel en México, pero muchos usuarios desconocen esto.

Los usuarios que reciben un correo como el de la imagen y envían el código solicitado, en realidad transfieren 93 pesos de su propio saldo al número XXXXXXXXXX. En este ejemplo hemos borrado el número de teléfono, pero debes saber que, sin importar qué número presenten, se trata de un fraude en el que debes evitar caer, sabiendo que ninguna compañía celular envía este tipo de mensajes y que, por supuesto, no te duplicará ningún saldo.

### ¿Cómo puede causarme daño un correo electrónico?

Además de la constante molestia que implica recibir decenas y hasta cientos de correos basura por semana, en la mayoría de los casos mencionados arriba los defraudadores que envían los correos buscan el lucro por medio de la estafa, intentan engañarnos para lograr obtener nuestro dinero o nuestra información confidencial para después hacer mal uso de ella, casi siempre con daño a nuestro patrimonio.

¿Cómo lo logran? A continuación presentamos las categorías de los casos recibidos en ASI a la fecha:

#### a) Ingeniería social

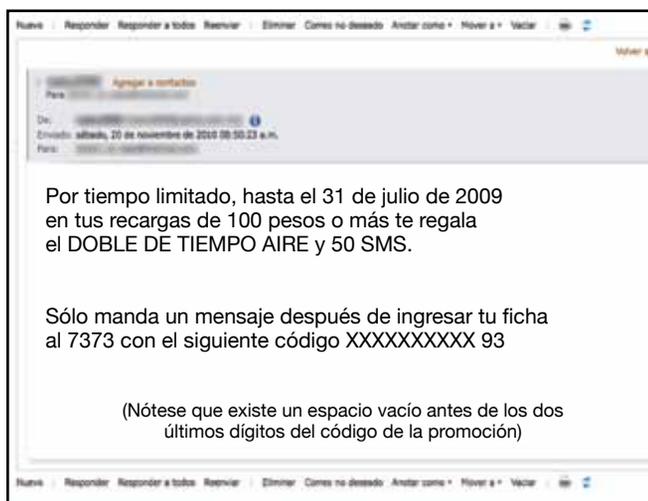


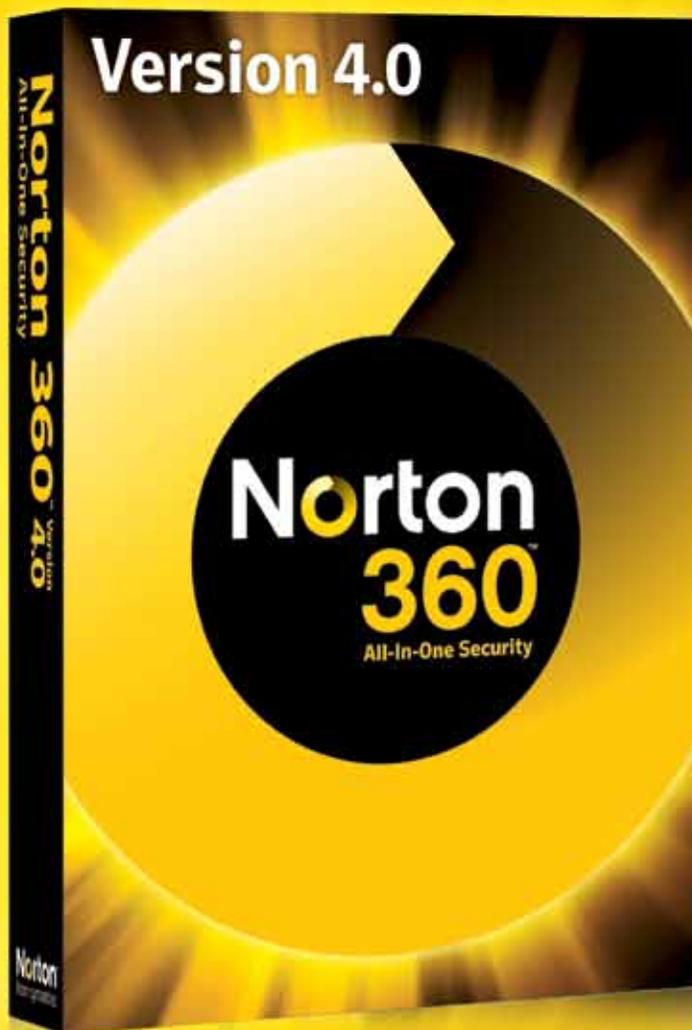
Fig. 1. Ejemplo de un correo que te invita a “duplicar tu saldo”.

#### b) Archivos adjuntos contaminados

El mensaje puede venir acompañado con archivos que contengan virus o código malicioso (malware). Si el usuario intenta abrirlos, su equipo se contamina automáticamente, a menos de que cuente con la protección actualizada.

Un ejemplo de lo anterior fue una serie de correos falsos que decían “Profeco informa”. Éste en realidad engañaba al usuario con un archivo adjunto supuestamente de la lista de las gasolineras donde se ofrecían litros completos de gasolina, pero que en realidad era malware (*malicious software*, o software malicioso) para espiar al usuario (ver más adelante “¿Cómo me puede afectar el malware?”).

# Seguridad Todo-En-Uno



- ✓ Antivirus
- ✓ Protección contra spyware
- ✓ Protección contra bots
- ✓ Protección mediante firewall
- ✓ Protección de la red
- ✓ Optimización del equipo
- ✓ Protección para el navegador
- ✓ Soporte gratuito ilimitado

**Cada click importa.**

Protección rápida y ligera contra las amenazas para la seguridad del equipo.



### c) Redirección a páginas falsas

Con cualquier pretexto, un correo electrónico puede tratar de engañar al usuario para lograr que visite una página fraudulenta. Al momento de visitarla, la página puede intentar sembrar código malicioso (malware) en el equipo, o bien, presenta un formulario solicitando información confidencial del usuario, como nombre completo, dirección y números de tarjetas de crédito.

Un engaño muy común en estas páginas es que presentan un mensaje que informa al usuario que “para visualizar la página se requiere instalar la última versión de Adobe Flash player” y pide permiso para instalarlo (como si fuera muy legal). La realidad es que la aplicación intentaría sembrar código malicioso en el equipo.

El caso más común de este tipo de engaños es el conocido como “Phishing bancario”, en donde el usuario recibe un correo con un texto similar a éste:

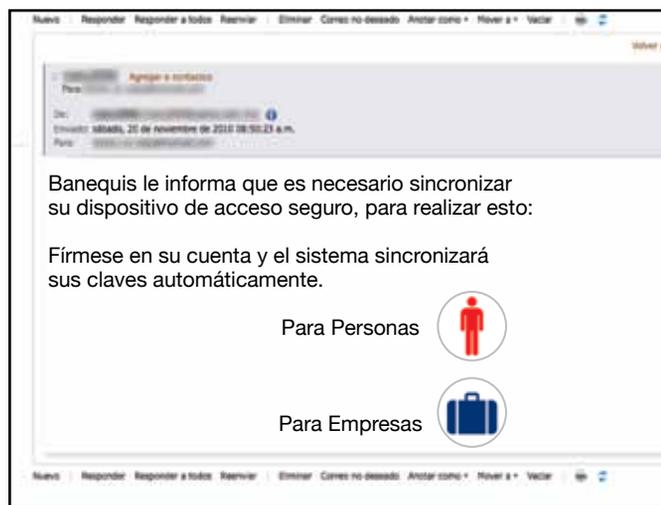


Fig. 2. Modelo de un correo que te enviaría el supuesto banco “Banequis”.

Si el usuario hace clic sobre la imagen de “Para Personas” o “Para Empresas”, es redirigido a una página que intentará sembrar código malicioso o solicitará información confidencial.

Si bien el primer caso utiliza ingeniería social pura, en los dos restantes también se utiliza para manejar historias convincentes que engañen al usuario para lograr que abra los archivos adjuntos o que visite la página fraudulenta.

### ¿Cómo me puede afectar el malware si llega a mi computadora?

Como mencionamos antes, el *spam* es un vehículo



para conducir código malicioso (malware) hasta tu computadora. Como se vio en los ejemplos mostrados, varios de los esquemas de engaño buscan sembrar malware para diferentes propósitos. Aquí te presentamos los más comunes para que comprendas la importancia de mantener tu equipo protegido con software de seguridad:

### SPYWARE

Puede espiar y guardar registro de los sitios que visitas para informarlo al creador del código sin que te des cuenta.

### VIRUS, TROYANOS Y GUSANOS

Que pueden utilizar tu máquina en centro de envío de correos basura (*spam*) o utilizarla para atacar a otros usuarios o sitios de Internet (a esto se le llama convertirla en “bot” o zombi), localizar información confidencial en tu equipo, e incluso, destruir información irremediablemente.

### BACKDOORS

Abre un puerto de tu equipo para que el autor del malware pueda controlarlo, instalarle otros códigos, usar los recursos del equipo, etcétera.

### DIALERS

Hacen llamadas a números de paga con cargo al recibo del usuario, esto sólo aplica en conexiones dial-up.



## KEYLOGGERS

Registran todo lo que se escribe en el teclado de la computadora, almacenándolo en archivos ocultos que después son enviados al autor del malware. Esto puede incluir desde nombres de usuario, contraseñas, números de cuenta, o incluso hasta correos y documentos personales, es decir, todo lo que el usuario escriba.

No es difícil imaginar el mal uso de tu propia información una vez que el autor del malware la recibe por cualquiera de estos métodos. Existen muchos otros tipos, sin embargo, éstos son los más comunes. Si te interesa conocer información de otras variantes también peligrosas, te invitamos a consultar el siguiente artículo en Wikipedia, donde se explica lo que es el adware, exploits, hoaxes, rootkits, etcétera:

<http://es.wikipedia.org/wiki/Malware>

2

## RECOMENDACIONES DE PREVENCIÓN

Es prácticamente imposible “blindar” tu dirección de correo para que no caiga en manos de un *spammer*, por lo que una buena sugerencia práctica es que utilices una cuenta de correo anónima para participar en foros, registrarte en sitios web, etcétera, y utilices otra dirección de correo electrónico para mensajes relacionados con tu trabajo o asuntos serios, y nunca la ofrezcas en formularios de sitios como entretenimiento y turismo. Si te das cuenta, el hecho de que un *spammer* tenga tu dirección de correo no sería tan grave si ésta no se encuentra asociada a datos que puedan identificarte en el

mundo real, como tu nombre y dirección postal.

Y por supuesto es recomendable que actives un filtro antispam, prácticamente todos los manejadores de correo cuentan con esta opción, como Mac Mail y Outlook, incluso los que son basados en Internet, como Yahoo y Gmail, pero frecuentemente está deshabilitado.

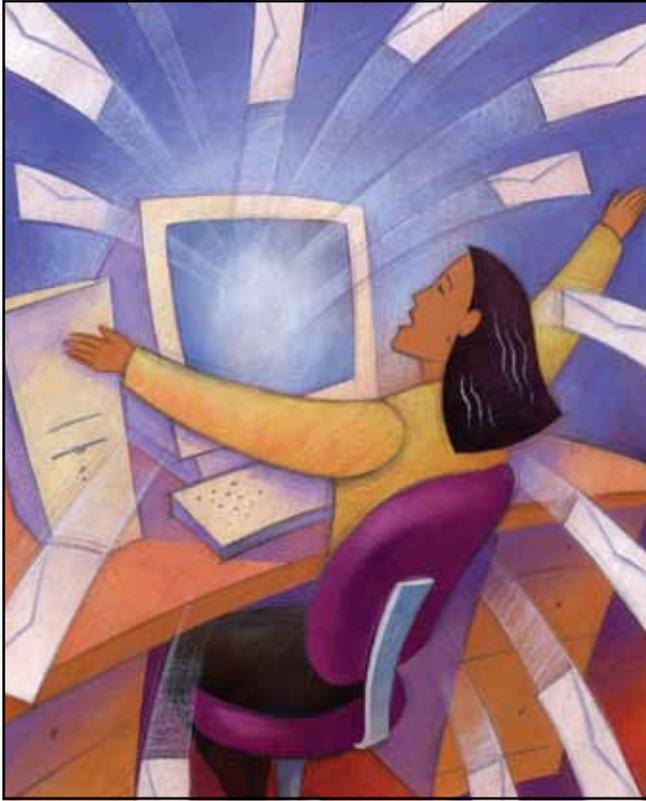
Estos filtros se encargan de revisar aspectos técnicos de los correos que reciben para determinar si son válidos o no. Si determinan que son correos no solicitados o *spam*, los envían a un buzón de correo basura.

Ejemplos de aspectos técnicos a revisar:

- Demasiadas palabras como “gratis” y “free” en el asunto o en el mensaje.
- Imágenes con ligas.
- Discrepancias entre la dirección del remitente y el valor en “Responder a:”, etcétera.

Es importante mencionar que estos filtros no son infalibles, por lo que la precaución debe persistir, y en un número mínimo de ocasiones, un correo válido puede ser depositado en el buzón de correo basura, por lo que es conveniente revisarlo de vez en cuando.





A la fecha de esta publicación, lamentablemente el *spam* no es considerado ilegal en México. Sin embargo, esto tampoco sería una solución definitiva. En Estados Unidos, en donde sí es ilegal, se genera más del 40% del *spam* mundial, es decir, hablamos de miles de millones de correos, que ninguna autoridad podría realmente contener. En el próximo ejemplar presentaremos la sección “¿Es delito el *spam* en México?”, para que conozcas el marco legislativo vigente al cual podrías recurrir en caso necesario.

Existen muchas formas en que los *spammers* pueden conseguir lotes de correos electrónicos en donde fácilmente puede estar incluida la tuya. No dejes de revisar el artículo “¿Por qué te llegan correos no solicitados?” en el siguiente número.

Finalmente, algo que siempre funciona a favor del usuario, es incorporar máxima precaución y sentido común sobre los mensajes que se reciben.

Recuerda, todos estos intentos de estafa o fraude aprovechan la facilidad que ofrece Internet para contactar a millones de usuarios, suplantando la identidad del remitente. Internet es sólo un medio de comunicación, el fraude nace en la mente del defraudador, y no con la tecnología.

Al igual que en el mundo real, en Internet nadie regala nada a cambio de nada. Aquí te ofrecemos algunos consejos o puntos a revisar en un correo para identificar si se puede tratar de un engaño.

- Si no solicitaste el correo, desconfía.
- Si el correo solicita información personal, o que llenes un formulario, no lo hagas.
- Si el correo tiene ligas, ya sea en texto o imágenes, ten mucha precaución y cerciórate primero a dónde te llevará esa liga.
- Los mensajes con múltiples faltas de ortografía frecuentemente son intentos de engaño.
- Desconfía de ofertas “maravillosas”.
- Suelen tener algún texto de urgencia para invitarte a que actúes de inmediato.
- Recuerda que empresas serias nunca te solicitarán información por correo electrónico.
- Nunca respondas mensajes que te indican que ganaste un premio o una lotería, siempre son falsos.

Debes saber que usuarios mexicanos han perdido dinero por hacer caso a este tipo de correos, como en el ejemplo que presentamos en el ejemplar anterior, por lo tanto, ninguna precaución está de más.

3

### MODUS OPERANDI

La Unidad de Investigación Cibernética de la PGJDF nos comparte información sobre la forma en que los delincuentes se aprovechan de la tecnología para tratar de engañarte. Conociendo estos modus operandi puedes identificar cualquier intento en tu contra y apartarte del riesgo.





En esta ocasión, nos describen un esquema basado en ofertas falsas de colaboración laboral, que con frecuencia tienen como objetivo a los jóvenes que escriben blogs, o bitácoras digitales:

1. El delincuente publica diferentes ofertas de empleo, casi siempre dirigido a personal femenino, en periódicos y en sitios de Internet.

Adicionalmente, visitan blogs publicados por jóvenes, les dejan un mensaje felicitándolos por lo bien que escriben, y los invitan directamente a ganar el puesto aprovechando su habilidad.

2. Una vez que la víctima observa la oferta y le interesa, se comunica por medio de correo electrónico.

3. Posteriormente inician una conversación, intercambian correos electrónicos y realizan una cita de trabajo.

4. Al llegar al lugar, se le pide a la víctima entrar a una sala en donde será evaluado junto con los demás “candidatos” citados, pero se le indica que debe dejar sus objetos o pertenencias en la recepción.

Una vez que todos los candidatos ingresan a la sala, uno de los delincuentes simula iniciar una plática introductoria para el “empleo”, mientras tanto,

otros integrantes toman todas las pertenencias recolectadas y se retiran del lugar. Unos minutos después, la persona que está fungiendo como instructor se disculpa un momento para salir de la sala con cualquier pretexto, por ejemplo, para traer un proyector e iniciar la presentación, pero al salir de la sala ya no regresa.

5. Al pasar un tiempo sin que nadie regrese a la sala, las víctimas se dan cuenta del engaño, pero es demasiado tarde.

6. Los datos con los que se identifican los probables responsables son falsos, tanto los que les llegan a mostrar a las víctimas, como los que utilizan para rentar las oficinas o espacios en donde citan a los incautos.

Por todo lo anterior, es importante que conozcas la forma en que este delito se comete para que aprendas a identificarlo y mantenerte apartado de convertirte en víctima. Es recomendable que se lo comentes a tu familia y demás personas que pienses que pueden estar expuestos.

Tu denuncia en [www.asi-mexico.org/denuncia](http://www.asi-mexico.org/denuncia) nos ayuda a mantener una clasificación actualizada de los esquemas que se utilizan para engañar a los usuarios, y poner la información al alcance de todos para lograr un aprovechamiento de Internet libre de preocupaciones.

**Si deseas mayor información o quieres hacer cualquier comentario, escríbenos a [contacto@asi-mexico.org](mailto:contacto@asi-mexico.org), o puedes contactar directamente a la PGJDF:**

**Contacto UIC  
Red (55) 52-42-64-18, 64-20 y 64-24  
[gic@pgjdf.gob.mx](mailto:gic@pgjdf.gob.mx)**





# El rol de la escuela

Cada día son más los colegios que están pasando de la preocupación a la ocupación cuando se trata de enseñar a los alumnos el uso seguro y responsable de las tecnologías de información y comunicación (TIC).

**E**n foros internacionales se ha venido insistiendo en la importancia de involucrar a los menores de edad en las discusiones acerca del rol que ellos mismos tienen sobre su propia seguridad en el manejo de las TIC, por ello, con el apoyo entusiasta de una gran cantidad de escuelas, el pasado 16 de octubre realizamos el primer **FORO ESTUDIANTIL DE DEBATE SOBRE SEGURIDAD Y PRIVACIDAD EN INTERNET** con el tema:

## INTERNET SIN RIESGOS, ¿MITO O REALIDAD?

Este foro se realizó en las instalaciones del Colegio Peterson Cuajimalpa, en México, D.F. Te invitamos a ver algunas cápsulas del evento en [www.efectoInternet.org/videos](http://www.efectoInternet.org/videos)



El enorme éxito de este evento nos permite confirmar que los jóvenes tienen mucho que aportar para lograr un escenario de tranquilidad en el entorno familiar y escolar, basado en el respeto a los demás usuarios y a la aplicación de normas básicas de comportamiento social, que les permiten socializar armónicamente con el universo digital que los rodea.

Es recomendable que los colegios fomenten la realización de más foros de debate, pues son los espacios donde los jóvenes pueden libremente compartir experiencias, plantear diferentes puntos

de vista y **generar propuestas** con la finalidad de reconocer los riesgos, y con base en sus deberes y derechos, apoyar a padres de familia y autoridades escolares en la elaboración de recomendaciones sobre el aprovechamiento responsable de las TIC.

Se llaman FOROS DE DEBATE porque se escuchan todas las opiniones y realmente se toman en cuenta. No se confrontan facciones en discusiones agotadoras, al contrario, se abren espacios para la libre expresión de ellos, que son los usuarios más activos y dinámicos de esta importante herramienta de la humanidad, y los resultados son verdaderamente gratificantes y de gran valor.

**Con la asistencia de más de 450 padres de familia, hijos y profesores, 56 alumnos representantes de escuelas públicas y privadas, integrantes del programa CENETIC Escolar, reunidos en el evento más importante sobre tranquilidad en Internet para las familias mexicanas, hubo ideas y se debatieron temas**

**basados en los resultados de la encuesta de seguridad y privacidad web aplicada por la A.S.I. entre más de 5000 alumnos.**

**En A.S.I. queríamos demostrar que un evento sobre seguridad en Internet no tiene por qué ser rígido y solemne. La misión del foro era ofrecer un espacio para que toda la familia pudiera estar presente, por lo que se ofrecieron actividades para todas las edades.**

**Hubo excelentes comentarios de los asistentes. Aquí citamos uno que sintetiza el objeto, misión y alcance de este evento:**

**“Donde nosotros vemos riesgos, ellos ven diversión, por eso...”**

**...las conclusiones del debate entre alumnos nos dejan ver con claridad los pasos que debemos tomar en casa y colegios. Sería un error no poner atención a este mensaje”.**



Excelentes instalaciones



Enorme interés



Actividades complementarias



Diferentes planteles, gran compañerismo



Rally de la SSP



### PUNTOS PRINCIPALES DEL FORO:

#### 1. EL DEBATE ENTRE ESTUDIANTES.

Conducido por el Dr. Alejandro Nagy, con el apoyo de la Dra. Brenda Morales y la Mtra. Paola López, ofreció una oportunidad única para conocer sus puntos de vista sobre varios resultados de la encuesta de seguridad y privacidad web que habían generado preocupación entre padres de familia y autoridades académicas, por ejemplo:

- **26% acuden a encuentros con extraños.**
- **50% ofrecen acceso irrestricto a su información a todo aquel que consideran un “amigo”.**
- **17% conocen personas que han enviado imágenes de desnudos de sí mismos.**

La participación de los alumnos fue entusiasta, y las posturas manifestadas nos enseñan la necesidad de un trabajo intensivo en aspectos familiares, psicológicos y sociales, ya que por el momento rechazan la idea de que sus padres aprendan más sobre tecnologías para involucrarse con ellos y no



reconocen la autoridad de la escuela para sancionar sus conductas aun cuando afecten a miembros de la comunidad escolar, si éstas fueron cometidas fuera del plantel.

#### 2. EL MÁS COMPLETO PROGRAMA DE CONFERENCIA PARA LOS PADRES DE FAMILIA Y PROFESORES.

**9:45**  
**Presentación especial.**

**Tecnología en el salón de clases.** Realizada por alumnos de la carrera de Informática Administrativa de la Escuela Bancaria y Comercial, demostraron cómo los medios digitales tienen un lugar relevante en la enseñanza moderna.



#### CONFERENCIAS:

**10:30**  
**Presentación especial:**

**“El rol de Internet en la trata de niños, niñas y adolescentes en México”.**

A cargo de la diputada Rosi Orozco, presidenta de la Comisión Especial para Combatir y Sancionar la Trata de Personas.

**Con el testimonio presencial de una menor sobreviviente de la trata.**



11:30

**Sesión especial:**

**Presentación del proyecto ciudadano  
"Mapa Delincencial"**

por parte de las ONG miembros del comité directivo.



12:00

**"Las nuevas tecnologías: ¿nos dirigimos  
a la salvación o a la condenación del  
mundo moderno?".**

Dr. Enrique Tamés M., Tecnológico de Monterrey.



**Receso coffee break.**

13:30

**"Seguridad en la navegación en línea, ¿sueño o  
realidad?".**

Ing. Rafael A. García Ladrón de Guevara, gerente regional de Producto para América Latina. Symantec Corporation México.



14:30

**"Los delitos cibernéticos y sus modus operandi".**

A cargo de la Policía Cibernética del D.F. y FEVIMTRA, a cargo de la fiscal Mtra. Sara Irene Herrerías, ponencia sobre los servicios que ofrece a la sociedad, con énfasis en delitos originados en Internet.



### 3. ACTIVIDADES COMPLEMENTARIAS:

Para fomentar la asistencia de toda la familia, se ofrecieron interesantes actividades complementarias que los hijos acompañantes pudieron disfrutar:



#### CONVIVENCIA CON LA SSP

Gracias al apoyo de la Subsecretaría de Prevención del Delito, contamos con la presencia de una patrulla de la Policía Federal, con la que los oficiales explicaron a los menores de edad y público interesado el equipo que utilizan para desarrollar su importante labor, algunos de sus procedimientos y responsabilidades, lo que ofreció una oportunidad única a los asistentes para acercarse a la autoridad y entender los riesgos que implica el combate a la delincuencia.

#### RALLY CONTRA EL DELITO CIBERNÉTICO

Por medio de actividades recreativas organizadas por la SSP, los jóvenes aprenden a protegerse del delito cibernético en modalidades como narcomenudeo y explotación infantil. Las actividades incluyen competencias, creación de porras, desarrollo de mensajes de prevención y mucho entretenimiento lúdico.



#### FUTBOL SOCCER

Para todos los niños y niñas que asistieron al evento, por parte de la escuela del Pachuca F.C., actividad que naturalmente atrajo la atención y les permitió pasar un día agradable a los menores que acompañaron a sus padres, y que reforzó en los padres de familia la importancia de equilibrar las actividades digitales de sus hijos con tareas físico-recreativas.



#### 4. STANDS PARA ENSEÑANZA DE TECNOLOGÍAS DE PUNTA.

Las empresas patrocinadoras ofrecieron servicios durante los recesos para mostrar a los asistentes cómo sus tecnologías pueden responder a las necesidades de protección de los menores, atendiendo a preguntas concretas para obtener el máximo provecho de los productos mostrados, con lo que aprovecharon doblemente su asistencia a este evento.



Stand Tec de Monterrey



Stand PC Tools



Stand Telmex

#### 5. INFORME DE CONCLUSIONES.

El documento de conclusiones y recomendaciones del debate estudiantil completo se pondrá a disposición de los colegios miembros del programa CENETIC Escolar, y un resumen de los aspectos más relevantes está a disposición de entidades educativas y público en general. Se puede solicitar enviando un correo a [contacto@asi-mexico.org](mailto:contacto@asi-mexico.org)

Si te interesa que tu escuela sea parte del programa CENETIC Escolar, envíanos un correo a [escuelas@asi-mexico.org](mailto:escuelas@asi-mexico.org) para remitirte todos los detalles.

**ESTE IMPORTANTE EVENTO FUE PATROCINADO POR:**



**CON LA PARTICIPACIÓN DE:**



Y la convocatoria de:

**Colegios Peterson, Colegio Nuevo Continente, Colegio Robert Schuman, The Churchill School, Instituto Piaget, Instituto La Paz, Colegio Gandhi, Instituto Técnico y Cultural, Colegio Ameyalli, Colegio Cemie y varios colegios invitados.**

WiFi  móvil en  
**infinitem**  
La conexión más rápida



**WiFi**  
**GRATIS**



Conéctate gratis con **WiFi Móvil en infinitem** desde tu laptop, iPad, iPhone o smartphone con conexión **WiFi**. Navega sin cables en parques, restaurantes, aeropuertos, cafeterías, universidades **y más de 3,900 lugares** siempre con la conexión más rápida en **infinitem**.

Llama al **01 800 123 2222** para obtener tu password

Consulta los sitios en: [telmex.com/infinitemmovil](http://telmex.com/infinitemmovil)

 **TELMEX**  
está contigo