EFECTO INTERNET

www.asi-mexico.org

Tranquilidad en la era digital
para aprovechar al máximo la red

Alianza por la SEGURIDAD en Internet

Vol. 0, No. 0 / Junio de 2010

Mejores practicas para tu celular

Internet alternativo

Sólo
SEGURIDAD TELCEL
protege tu computadora con:

Antivirus Telcel + Disco Virtual Telcel

Para que navegues sin preocuparte.

- Antispyware
- Antispam
- Firewall y más

Para que almacenes y compartas tus archivos en la Web.

- Respaldo automático

Básico

Antispyware
Antivirus
Antispam
Protección de navegación
Herramientas de recuperación
Actualizaciones
Disco Virtual Telcel 1 GB

$39.00 al mes

Profesional

Paquete Básico
+
Firewall
Disco Virtual Telcel 5 GB

$49.00 al mes

Seguridad Total

Paquete Profesional
+
Control parental
Protección de identidad
Respaldo automático
Disco Virtual Ilimitado

$99.00 al mes

Contrata el paquete que se adapte a tus necesidades y llévate un mes de servicio gratis. McAfee steek

Información en www.bat.telcel.com/seguridad.html Centros de Atención a Clientes y Distribuidores Autorizados.

www.telcel.com/bat

telcel M.R.

EFECTOINTERNET
www.asi-mexico.org

EDITORIAL

Tranquilidad en la era digital

Internet es una fantástica tecnología de información y comunicación, cuyo potencial ha transformado por completo la forma en que las nuevas generaciones se desenvuelven, se comunican, se divierten, aprenden, comparten, y que en conjunto, ha definido para ellos un nuevo concepto de "Socialización digital".

A los ojos de los Padres de Familia y de sus profesores, los jóvenes se la pasan "pegados" a todo el arsenal de dispositivos digitales que tienen a su disposición y que manejan a su antojo, como computadoras portátiles, iPods, Cámaras, Video consolas, teléfonos celulares, etc…, que los mayores desconocen y por ende los apartan de la posibilidad de orientar a sus hijos en temas como seguridad y privacidad, tan importantes en el desarrollo de todo niño, niña y adolescente.

Para la tranquilidad de los Padres de Familia en esta era digital, hay buenas noticias. El desarrollo de las nuevas tecnologías en Internet ha venido a demostrar, que lo importante no es el equipo que se utiliza, sino las actividades que se realizan. ¿Qué hacen los niños? ¿Con quién y de qué hablan en Internet? ¿Qué relaciones construyen? ¿En qué comunidades participan? Cuestiones en las que los podemos orientar con parentalidad tradicional para su sano desarrollo.

Muchas veces hemos escuchado a los adultos explicar que no se acercan a lo que hacen sus hijos en Internet porque no conocen de computadoras. Esto ya no tiene porque ser un impedimento, ahora tenemos en México más del doble de teléfonos celulares con acceso a internet, que computadoras conectadas a la red, y casi todos los mayores cuentan con uno y lo saben utilizar.

A lo largo de esta guía, presentamos muchas ideas y recomendaciones que buscan darle a los Padres de Familia y a los Profesores, la tranquilidad para permitir que los menores aprovechen al máximo la tecnología a su disposición, de forma sana y responsable, siempre en su beneficio.

La tecnología es un vehículo de desarrollo para todos los países, no debemos pensar en apartar a las nuevas generaciones de su máximo aprovechamiento, solo debemos aprender a orientarlos para canalizarla siempre hacia usos positivos, productivos y constructivos, que les ayude a ser mejores individuos y por ende, mejor sociedad y país.

Internet por definición es una red de computadoras, pero en la práctica, es en el fondo una red de personas, de ideas, de conceptos, de información, de acceso a fantásticas oportunidades de comunicación, entretenimiento, educación, cultura y productividad, que está ahí para que todos la disfrutemos, esta guía te invita a descubrir su potencial y aprovecharlo al máximo, por eso te invitamos:

¡VIVE EL EFECTO INTERNET!
Comité Editorial
Alianza por la Seguridad en Internet A.C.
www.asi-mexico.org

ÍNDICE

INTERNET ALTERNATIVO

FireFox con "personas" 4
Google Chrome 5

INTERNET EN LA FAMILIA

Hable con sus hijos 6
Consejos para padres de niños de diferentes edades 7
Socialización en Línea 9
Comunicación en Línea 12
Teléfonos Móviles, Socialización y Comunicación en movimiento 14
Proteja su computadora 16
Controles paternos 18
Proteja la privacidad de sus hijos preadolescentes 20
El rol de la escuela 22

INTERNET PRODUCTIVO

Banca en línea 27

INTERNET BIBLIOGRÁFICO

En esta edición recomendamos 30

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 alternativo

¡En esta sección conocerás nuevas alternativas para disfrutar Internet a tu manera!

"En la variedad está el gusto", nos dice un popular refrán Mexicano. En internet, ¡en la variedad está también la diversión! Tú puedes hacer más divertida tu experiencia en internet, personalizando a tu gusto tu navegador, con la máxima seguridad.

Mozilla Firefox con "personas"

¡Y vístelo con la imagen que más te guste!, conoce **Firefox PERSONAS, visita www.getpersonas.com** y escoge entre más de 35,000 diseños para personalizarlo, o bien, crea tu propio diseño y compártelo con el mundo:

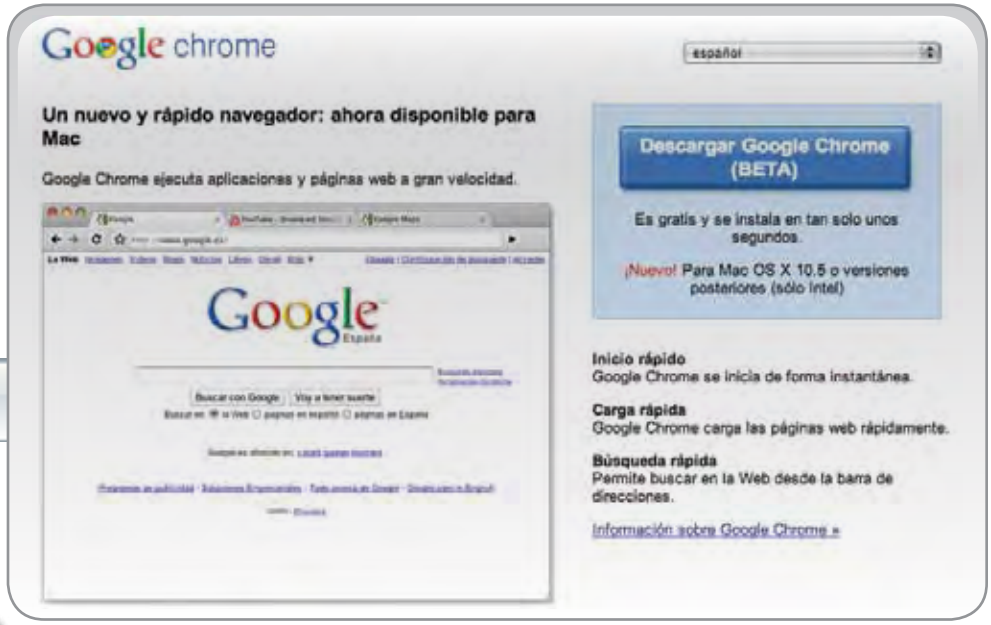
¿LE VAS A UN GRAN EQUIPO DE FUTBOL?

¿TE ENCANTAN LOS CARROS DE GRAN LUJO?

¿TE GUSTAN LOS DEPORTES EXTREMOS?

Google Chrome

Para usuarios que prefieren un entorno minimalista y gran **velocidad** en el despliegue de páginas de internet.



Descarga **gratis** la última versión en **www.google.com/chrome.**

Hasta la barra de navegación es única. Llamada **Omnibox,** sirve para todo.

OMNIBOX:

Un navegador que ofrece simplicidad y alto rendimiento. Con una interfase limpia y minimalista, que no presenta ni un menú tradicional. Hasta la barra de navegación es única. Llamada Omnibox, sirve para todo: desde teclear las direcciones de las páginas web, buscar palabras en Google, e incluso, revisar el historial de sitios visitados.

¿Quieres gran velocidad?
Chrome incorpora el motor gráfico WebKit, considerado el más rápido, y también una versión especial de Java Script que es sumamente veloz. En las pruebas, la carga de páginas web convencionales es muy rápida, pero los servicios y aplicaciones web modernos, muchos de la propia Google (GMail, Google Maps, etc…) se benefician enormemente.

¿TE GUSTA JUGAR AL AGENTE SECRETO?

¿NO QUIERES QUE NADIE SEPA LAS PÁGINAS QUE VISITAS?

Navegando en **"modo incógnito"** las páginas visitadas no se registran en el historial de navegación.

DISFRUTA Y VIVE EL EFECTO INTERNET ALTERNATIVO

© Información de Copyright. Toda las marcas, logos y nombres comerciales son propiedad de sus titulares.

internet en tu familia

En esta sección encontrará información útil que le permitirá acercarse a las actividades en línea de sus hijos.

Tome en cuenta que la Seguridad en Internet se basa principalmente en medidas de sentido común, muy similares a las que tomamos en el mundo real para andar tranquilos por las calles. Platique con tus hijos para orientarlos y lograr que tengan experiencias muy positivas, sobre todo ahora que tienen a su alcance todo tipo de dispositivos digitales que les permiten permanentemente comunicarse, divertirse, aprender y compartir.

Estas formas de socializar y comunicarse pueden ser convenientes y agradables, pero vienen acompañadas de riesgos, algunos son:

CONDUCTA INAPROPIADA.

El mundo en línea puede dar la sensación de anonimato. A veces los niños se olvidan que continúan siendo responsables de sus acciones.

CONTACTO INAPROPIADO.

En línea hay algunos individuos con malas intenciones, entre los que se incluyen los acosadores, intimidadores, depredadores, hackers y estafadores.

CONTENIDO INAPROPIADO.

Puede que esté preocupado por los contenidos pornográficos y violentos, el lenguaje obsceno o los insultos que sus hijos pueden encontrar en línea.

Usted puede reducir estos riesgos hablando con sus hijos sobre la manera en que se comunican en línea y fuera de línea—y alentándolos a actuar de una manera que los enorgullezca.

Esta guía cubre lo que usted necesita saber, dónde recurrir para consultar más información y temas de conversación para tratar con sus hijos sobre cómo vivir sus vidas en línea.

¿Hable con sus hijos

¿Cuál es la mejor manera de proteger a sus hijos mientras están en línea?

Hablando con ellos.

Los investigadores indican que cuando los niños quieren obtener información importante, la mayoría de ellos confía en sus padres.

► ¿TIENE DUDAS SOBRE CÓMO EMPEZAR LA CONVERSACIÓN?

CONSIDERE LO SIGUIENTE:

► COMIENCE A TEMPRANA EDAD.

Después de todo, incluso los niños que recién comienzan a caminar ven que sus padres utilizan todo tipo de aparatos. Tan pronto como su hijo comience a usar una computadora, un teléfono celular o cualquier aparato móvil o portátil, es el momento indicado para hablar con él sobre cómo comportarse cuando está en línea y sobre la protección y la seguridad. Como padre, usted tiene la oportunidad de hablar con su hijo sobre estas cuestiones importantes antes de que lo haga otra persona.

► CREE UN AMBIENTE SINCERO Y ABIERTO.

Los niños observan a sus padres como sus propios guías. Sea comprensivo y positivo. Escucharlos y tomar en cuenta sus sentimientos los ayuda a mantenerse atentos a la conversación. Es posible que usted no tenga todas las respuestas, y admitirlo sinceramente puede ser de gran ayuda.

► INICIE LA CONVERSACIÓN.

Aunque sus niños se acerquen espontáneamente para hablar con usted, no espere a que sean ellos los que inicien la conversación. Aproveche las oportunidades que se presentan a diario para hablar con sus hijos sobre

cómo actuar cuando están en línea. Por ejemplo, un programa de TV en el que aparece un adolescente navegando en línea o usando un teléfono celular puede presentar una oportunidad para hablar sobre qué es lo que se debe—o no se debe—hacer en una circunstancia similar. Por ejemplo, las noticias sobre estafas en internet, casos de ciber-acoso o ciber-violencia, también pueden servir para comenzar una conversación con los chicos sobre sus experiencias y sus propias expectativas.

▶ COMUNIQUE SUS VALORES.

Sea directo sobre sus valores y de qué manera se aplican dentro del contexto en línea. Comunicar sus valores de manera clara puede ayudar a sus hijos a tomar decisiones más inteligentes y meditadas cuando se enfrentan a situaciones delicadas.

▶ TENGA PACIENCIA.

Resista las ganas de forzar la conversación con sus hijos. La mayoría de los chicos necesita que se le repita la información, en pequeñas dosis, hasta que logran incorporarla. Si sigue hablando con sus hijos, se verá recompensado a largo plazo por su paciencia y persistencia. Haga un esfuerzo para mantener abiertas las líneas de comunicación, incluso cuando sepa que su hijo hizo algo en línea que usted juzga inapropiado.

Consejos para padres de niños de diferentes edades

El contacto masivo de los menores con la tecnología está modificando en diversas formas su desarrollo, haciendo ya que los limites de edades que normalmente definen cada etapa de sus vidas no siempre sean tan claros. Los padres de familia saben mejor que nadie como definirían a sus hijos, dentro de alguna de estas categorías:

- NIÑOS PEQUEÑOS
- PREADOLESCENTES
- ADOLESCENTES

▶ NIÑOS PEQUEÑOS

Cuando los niños pequeños comienzan a usar una computadora, deben estar supervisados de cerca por un padre o por la persona a cargo de su cuidado. Desde el comienzo, es conveniente que los padres elijan los sitios Web que pueden visitar sus hijos—y que no los dejen navegar a otros sitios solos. Si no se supervisa a los niños pequeños mientras navegan en línea, estos podrían tropezar con sitios que pueden asustarlos o confundirlos.

Cuando usted piense que su chiquito ya está preparado para explorar por su propia cuenta, es importante que usted esté cerca cuando vaya de un sitio a otro. Puede que quiera restringirle el acceso a sitios que usted ya ha visitado y sabe que son apropiados para la edad—por lo menos en lo que se refiere a su valor educativo o de entretenimiento.

▶ PREADOLESCENTES

Durante la etapa preadolescente los niños comienzan a explorar con más independencia, pero esto no significa que usted no quiera —o no necesite—estar a mano.

Es importante estar con ellos—o por lo menos cerca de ellos—cuando están en línea. Si tiene hijos preadolescentes, considere instalar la computadora en un lugar de la casa en el cual el niño esté cerca de usted o de otro adulto. De estamanera, pueden ser “independientes”, pero no estarán solos.

Las funciones de control paterno—filtros o herramientas de monitoreo—pueden resultar efectivas para los más chicos de este grupo. Pero, hay muchos chicos de esta edad que ya tienen los conocimientos técnicos necesarios para encontrar una manera de esquivar los controles. Si hasta ahora los chicos no habían comenzado a navegar por internet para hacer las tareas de la es-

cuela, es probable que sea el momento en que empiecen a hacerlo. También es el momento en el cual pueden descubrir recursos para sus pasatiempos favoritos y demás intereses. Muchos preadolescentes son adeptos a la búsqueda de información en línea. Con frecuencia, ésta es una tarea útil para el resto de la familia, pero siguen necesitando del consejo de un adulto que los ayude a entender cuáles son las fuentes confiables.

Cuando considere qué es lo que sus hijos preadolescentes pueden hacer y ver en internet, piense también cuánto tiempo pasan en línea. Considere la posibilidad de establecer límites para la frecuencia y duración de sus sesiones de navegación en internet.

▶ ADOLESCENTES

Los preadolescentes tienden a reflejar los valores de sus padres. Cuando comienzan la adolescencia, los jóvenes ya están formando sus propios valores y comienzan a adoptar los valores de sus pares. Al mismo tiempo, los adolescentes más grandes están madurando física, emocional e intelectualmente, y muchos de ellos están ansiosos por experimentar una mayor independencia de sus padres.

Los adolescentes tienen un mayor nivel de acceso a internet a través de sus teléfonos celulares, aparatos portátiles o desde las computadoras de sus amigos, y también tienen más tiempo disponible para ellos. Por lo tanto, no es realista pensar que usted puede estar en el mismo cuarto que sus hijos adolescentes mientras que están en línea. Es necesario que ellos sepan que usted u otro miembro de la familia puede entrar y salir de su cuarto en cualquier momento y preguntarles qué están haciendo en línea.

Con los adolescentes es importante enfatizar el concepto de credibilidad. Hasta los chicos más expertos en tecnología necesitan comprender que no todo lo que ven en internet es real, que en internet las personas pueden ser distintas de lo que aparentan ser, que la información o imágenes que comparten en línea pueden ser vistas por todas partes, y que una vez que colocan algo en línea es casi imposible “sacarlo”.

Como no se pueden ver las expresiones faciales, ni el lenguaje corporal u otras claves visuales en las que confiamos fuera de internet, los adolescentes pueden sentir que en línea tienen la libertad de hacer o decir cosas que no harían de otro modo. Recuérdeles que detrás de los nombres de pantalla, perfiles y avatares hay personas de carne y hueso con sentimientos reales.

Cuando hable con su hijo adolescente, establezca expectativas realísticas. Anticipe cuáles serán sus reacciones si descubre que ha hecho algo en línea que usted desaprueba. Si su hijo adolescente le confía que vio en línea algo feo o inapropiado, intente tratar el tema con él para evitar que vuelva a suceder. Como su hijo adolescente se convertirá pronto en un adulto, necesita saber cómo comportarse y cómo actuar con prudencia para usar la red de manera segura, sin correr riesgos y de acuerdo a los principios éticos de su familia.

¿Socialización en línea

Los adolescentes y preadolescentes socializan en línea a través de sitios de redes sociales, salas de chateo, mundos virtuales y blogs.

Los chicos comparten fotos, videos, ideas y planes con amigos, con otras personas que comparten sus propios intereses, y en ocasiones, con el mundo entero.

La socialización en línea puede ayudar a los chicos a conectarse con amigos e incluso con sus familiares, pero es importante que usted ayude a sus hijos a navegar estos espacios de manera segura. Entre los peligros que acarrea la socialización en línea se pueden mencionar el hecho de compartir demasiada información, o exhibir fotos, videos o palabras que pueden dañar la reputación o herir los sentimientos de otra persona. Aplicar la lógica y sentido común del mundo real puede ser útil para minimizar las desventajas de la socialización en el mundo virtual.

¿QUÉ PUEDE HACER USTED?

▶ Recuérdeles a sus hijos que las acciones que tomen en línea pueden tener repercusiones.

Las palabras que escriben en línea y las imágenes que suben a los sitios tienen consecuencias fuera de internet.

▶ Explíqueles a sus hijos que solamente deben colocar en línea la información que usted y ellos deseen que sea vista por otras personas.

Aunque estén activadas las funciones de seguridad, muchas más personas de las que usted quiere que lo hagan pueden ver el perfil en línea de su hijo. Aliéntelos a reflexionar sobre el tipo de lenguaje que usan cuando están en línea y a pensar dos veces antes de subir fotografías y videos a su página o alterar fotos subidas por otra persona. Los empleadores, encargados de admisiones de las universidades, entrenadores deportivos, maestros, y la policía pueden ver lo que su hijo coloca en internet.

▶ Recuérdeles a sus hijos que una vez que colocan la información en línea, no la pueden quitar.

Aunque eliminen la información de un sitio Web, tendrán muy poco control sobre las antiguas versiones que queden registradas en las computadoras de otras personas que pueden ser circuladas en línea.

▶ Utilice las funciones de privacidad para limitar quien puede acceder y colocar información en el perfil de su hijo.

Algunos sitios Web de redes sociales, salas de chateo y blogs ofrecen funciones de privacidad muy efectivas. Hable con sus hijos sobre estas funciones de privacidad y sus expectativas con respecto a quien debería estar permitido a ver sus perfiles.

▶ Revise la lista de amigos de sus hijos.

Probablemente desee limitar la lista de “amigos” en línea a aquellas personas que su hijo conoce realmente.

▶ Hable con sus hijos sobre evitar conversaciones sexuales en línea.

Los resultados de las investigaciones demuestran que los adolescentes que no hablan de sexo con extraños tienen menos probabilidades de entrar en contacto con un acosador. De hecho, los investigadores han descubierto que generalmente los acosadores no se hacen pasar por niños o adolescentes, y que la mayoría de los adolescentes que son contactados por adultos desconocidos lo ven como algo que les da escalofrío. Los adolescentes deben ignorar o bloquear a este tipo de individuos sin dudarlo.

▶ Entérese de lo que están haciendo sus hijos.

Familiarícese con los sitios de redes sociales que usan sus hijos para entender mejor sus actividades. Si usted está preocupado porque piensa que su hijo se está comportando riesgosamente cuando está en línea, puede explorar los sitios de redes sociales que frecuenta para ver qué tipo de información está colocando.

▶ ¿Se están haciendo pasar por otro? Intente buscar por el nombre o apodo de su hijo, escuela, pasatiempos favoritos, grado que cursa o área de residencia.

▶ Dígales a sus hijos que si tienen alguna sospecha confíen en sus instintos.

Aliéntelos a que le cuenten si cuando están en línea se sienten amenazados por alg una persona o se sienten incómodos con algo que ven en la red. Puede ayudarlos a reportar sus inquietudes a la policía y al sitio de redes sociales. La mayoría de estos sitios incluyen enlaces para que los usuarios puedan reportar inmediatamente los comportamientos abusivos, sospechosos o inapropiados en línea.

▶ Dígales a sus hijos que no finjan ser otra persona.

Explíqueles a sus hijos que es inapropiado crear sitios, páginas o subir material que aparenta pertenecer a otra persona, como por ejemplo un maestro, un compañero de clase o un personaje inventado.

▶ Pídales que creen un nombre de pantalla (Pseudónimo) seguro.

Aliente a sus hijos a pensar en la impresión que pueden causar los nombres de pantalla. Un buen nombre de pantalla no debería revelar demasiada información sobre la edad, el lugar de residencia o género del usuario. Por razones de seguridad, los nombres que sus hijos utilicen para el chat no deberían ser iguales a los de sus domicilios de correo electrónico.

▶ Ayude a sus hijos a entender que información debería permanecer privada.

Explíqueles la importancia de no dar a conocer datos sobre sí mismos, sus familiares y amigos. El nombre completo, número de Seguro Social, domicilio, número de teléfono e información financiera familiar—como por ejemplo los números de las cuentas bancarias o de tarjeta de crédito— es información privada y debe seguir siéndolo.

▶ SEXTING

Enviar o reenviar fotos, videos o mensajes de sexo explícito desde un teléfono móvil es una práctica conocida como sexting, que es la abreviatura de las palabras sex y texting. Dígales a sus hijos que no lo hagan. Además de poner en riesgo su reputación podrían estar infringiendo la ley.

Cuando los adolescentes son concientes de las consecuencias hay menos probabilidades de que tomen la decisión equivocada.

▶ CIBER-ACOSO

El ciber-acoso es el acoso o intimidación en línea. Puede producirse por medio de un mensaje electrónico, mensaje de texto, en un juego en línea, o a través de comentarios difundidos en un sitio de redes sociales. Podría involucrar rumores o imágenes colocadas en el perfil de alguna persona o difundidos para que otros los vean, o crear un grupo o página para excluir a una persona.

Hable con sus hijos sobre el acoso o intimidación. Dígales a sus hijos que no pueden esconderse detrás de las palabras que escriben y las imágenes que difunden.

En las redes sociales y el internet no todo es lo que parece.

¿Sabes con quién **realmente** estás platicando?

Nunca es demasiado pronto para aprender a cuidar tu información

Aunque seas niñ@
tu información es muy valiosa

Scitum

por una cultura
de la seguridad de la información

www.scitum.com.mx

Los mensajes hirientes no solamente hacen sentir mal al destinatario sino también dan una mala impresión sobre quien los envía—y a veces puede resultar en el desprecio de los compañeros y castigo de las autoridades.

Pídales a sus hijos que le cuenten si ven un mensaje o imagen que circula en línea que los hace sentir amenazados u ofendidos. Si teme por la seguridad de su hijo, establezca contacto con la policía.

Lea los comentarios. Con frecuencia, el ciber-acoso involucra comentarios malvados y dañinos. De vez en cuando revise la página de su hijo para ver con qué se encuentra.

No reaccione. Si su hijo es blanco de un acosador cibernético, dígale que no responda a la provocación. Por lo general, los matones buscan la reacción de sus víctimas. En su lugar, aliente a su hijo a tomar medidas juntos para guardar la evidencia y a hablar con usted sobre el tema. Si persisten los actos de intimidación, muéstrele la prueba a las autoridades escolares o las fuerzas del orden locales.

Proteja sus perfiles. Si su hijo encuentra un perfil creado o alterado sin su permiso, contacte a la compañía que opera el sitio para que lo elimine.

Bloquee o elimine el nombre del acosador de la lista. Si el acosador ejerce amenazas por medio de mensajes instantáneos u otro servicio en línea que tiene una lista de "amigos" o "compinches", elimine el nombre del acosador de las listas o bloquee su nombre de usuario o domicilio de correo electrónico.

Ayude a detener el ciber-acoso. Si su hijo ve que alguna persona es víctima del ciber-acoso, aliéntelo a tratar de detenerlo evitando comprometerse o reenviando las amenazas y diciéndole al acosador que deje de hacerlo. Los investigadores dicen que por lo general, el acoso cesa bastante rápido cuando intervienen los amigos de la víctima para defenderla. Una manera de ayudar a eliminar las prácticas de intimidación en línea es reportarlo al sitio o red donde las observa.

Reconozca los signos de un ciber-acosador. ¿Podría su hijo ser el acosador? Busque indicios de comportamiento intimidatorio, como por ejemplo la creación de imágenes malvadas de otro chico.

Tenga presente que usted es un modelo para su hijo. Los chicos aprenden a copiar a los adultos que difunden rumores o que se comportan con descortesía.

Comunicación en línea

El correo electrónico, chat, IM, video llamadas y mensajes de texto son formas rápidas y convenientes de comunicarse.

Pero lo básico — **qué** decimos, **cuándo** lo decimos y **por qué** lo decimos — son iguales en línea y fuera de línea. La cortesía y el sentido común son partes importantes de toda comunicación, en cualquier lugar que se produzca.

¿QUÉ PUEDE HACER USTED?

▶ Hable con sus hijos sobre sus modales en línea.

La cortesía y la buena educación son importantes. Usted le enseña a sus hijos a ser educados en la vida real; hable con ellos sobre la importancia de comportarse educadamente también cuando están en línea.

El envío de mensajes de texto puede parecer rápido e impersonal, pero las palabras amables como "pls" y "grx" son de uso común en los mensajes de texto, para abreviar por favor y gracias.

Bajando el tono. Escribir un mensaje en letras mayúsculas, una larga serie de signos de exclamación o en tipografía muy destacada equivale a gritar. La mayoría de las personas no aprecia el griterío.

Cc: y Responder a todos: con cuidado. Sugiérales a sus hijos que resistan la tentación de enviar un mensaje a todos los contactos de su lista.

Evitar los mensajes o cartas en cadena. En el mejor de los casos, la mayoría de las cartas o mensajes en cadena son una molestia y en el peor de los casos son estafas. Muchas de estas cartas o mensajes acarrean virus o programas espía. Pídales a sus hijos que no los abran ni los reenvíen.

▶ Configure las preferencias de alto nivel de privacidad en las cuentas de IM y video llamadas de sus hijos.

La mayoría de los programas de IM permite que los padres controlen si las personas de la lista de contacto de sus hijos pueden o no ver sus estatus en IM, incluso si están o no en línea. En algunas cuentas de IM y correo electrónico los padres pueden determinar quién puede enviar mensajes a sus hijos, y pueden bloquear a aquellos no estén en la lista.

▶ Pregúnteles a sus hijos con quiénes se comunican en línea.

De la misma manera que usted quiere saber quiénes son los amigos de sus hijos fuera de línea, es conveniente que sepa con quién hablan en línea.

▶ Hable con sus hijos sobre la importancia de crear contraseñas sólidas para las cuentas de e-mail y la necesidad de proteger estas contraseñas.

Cuanto más extensa sea la contraseña, más difícil resultará descifrarla. La información personal, su nombre de usuario, palabras de uso común o letras adyacentes en el teclado no son contraseñas sólidas. Para proteger sus contraseñas, los chicos deben evitar compartirlas con terceros, incluso con sus amigos.

▶ Recuérdeles a sus hijos que protejan la información personal.

Los números de Seguro Social, números de cuenta y contraseñas son algunos ejemplos de los datos que deben mantenerse en privado.

▶ PHISHING

Phishing es el nombre utilizado en inglés para denominar una práctica fraudulenta que se produce en internet cuando los estafadores envían mensajes de correo electrónico, mensajes de aparición automática (pop-up) o mensajes de texto para engañar a las personas y sacarles información personal y financiera. Luego usan la información para cometer robo de identidad.

▶ Vea cómo usted — y sus hijos — pueden evitar una estafa de phishing:

No responda a los mensajes electrónicos, de texto o de aparición automática que soliciten información personal o financiera ni haga clic sobre los vínculos o enlaces incluidos en estos mensajes. Tampoco utilice la función copiar y pegar (cut and paste) para colocar el domicilio de un enlace en el navegador de internet.

▶ Por ejemplo, si quiere consultar una cuenta financiera, escriba el domicilio Web que figura en su resumen de cuenta.

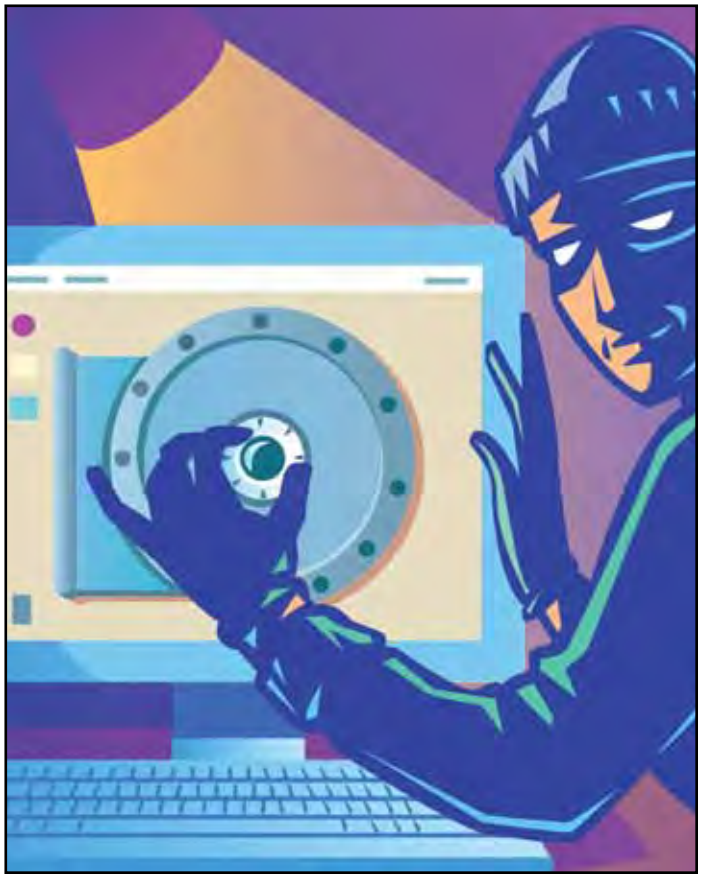
No dé información personal por teléfono en respuesta a un mensaje de texto. Algunos estafadores envían mensajes de texto que aparentan provenir de un negocio legítimo pidiéndole que llame a un número de teléfono para actualizar los datos de su cuenta o para acceder a un "reintegro". Si usted les facilita su información, la utilizarán para gastar en su nombre.

Tenga mucho cuidado al abrir o descargar los documentos o archivos adjuntados a los mensajes electrónicos recibidos, sin tener en cuenta quien sea la persona u organización que los envía. Estos archivos pueden contener virus o programas espías que el remitente desconoce.

▶ Use un programa de seguridad y actualícelo regularmente.

Lea la correspondencia que recibe; revise los resúmenes de sus tarjetas de crédito y cuentas bancarias tan pronto como los reciba para controlar que no le hayan imputado cargos no autorizados.

Reenvíe los mensajes electrónicos que parezcan fraudulentos a **denuncia@asi-mexico.org** y a la compañía, banco u organización invocada falsamente en el mensaje phishing.



Haga participar a sus hijos de estas actividades para que puedan desarrollar buenos hábitos de seguridad en internet. Comparta con ellos "momentos educativos"—si recibe un mensaje phishing, muéstreselos a sus hijos para ayudarlos a comprender que los mensajes que aparecen en internet no siempre son lo que aparentan ser.

Teléfonos moviles: socialización y comunicación en movimiento

¿Cuál es la edad apropiada para que un chico tenga un teléfono móvil? Esto es algo que debe decidir usted y su familia. Considere la edad de su hijo, su personalidad y madurez y las circunstancias familiares. ¿Es lo suficientemente responsable para cumplir las reglas que usted o la escuela establezcan para el uso del teléfono?

Muchas de las aplicaciones en línea también están disponibles en los teléfonos móviles—redes sociales, blogs, carga de contenidos, uso compartido de contenidos multimedia y edición de video. Enséñeles a sus hijos a tener en cuenta la seguridad cuando usan un teléfono celular.

¿QUÉ PUEDE HACER USTED?

► Dígales a sus hijos que si comparten fotos y videos por teléfono lo hagan con mucho cuidado.

La mayoría de los teléfonos móviles ahora vienen con cámaras de foto y video, lo cual facilita que los adolescentes fotografíen o graben cada momento y lo compartan desde cualquier parte.

Estas herramientas pueden fomentar la creatividad y la diversión; pero también presentan problemas relacionados con la reputación y seguridad personal. Aliente a sus hijos a pensar sobre su privacidad y las de los demás antes de compartir fotos y videos vía teléfono celular. Es fácil subir fotos y videos en línea sin el conocimiento—y mucho menos la aprobación—del fotógrafo o de la persona fotografiada. Puede ser abochornante e incluso riesgoso. Es más fácil pensárselo bien antes de compartir contenidos que controlar los daños luego.

► No tolere el uso del teléfono móvil para intimidar o acosar a otros.

Los teléfonos móviles pueden utilizarse para intimidar o acosar a otras personas. Hable con sus hijos y dígales que traten a los demás de la misma manera que quieren que los traten a ellos. Los buenos modales y los principios éticos que le ha enseñado también se aplican a sus comunicaciones telefónicas.

► Tenga buen juicio con respeto a las redes sociales móviles.

Muchos sitios de redes sociales permiten que los usuarios accedan desde sus teléfonos para revisar sus perfiles y colocar comentarios desde cualquier parte. Esto significa que los filtros que instaló en la computadora de su casa no limitarán las actividades de los chicos desde un teléfono.

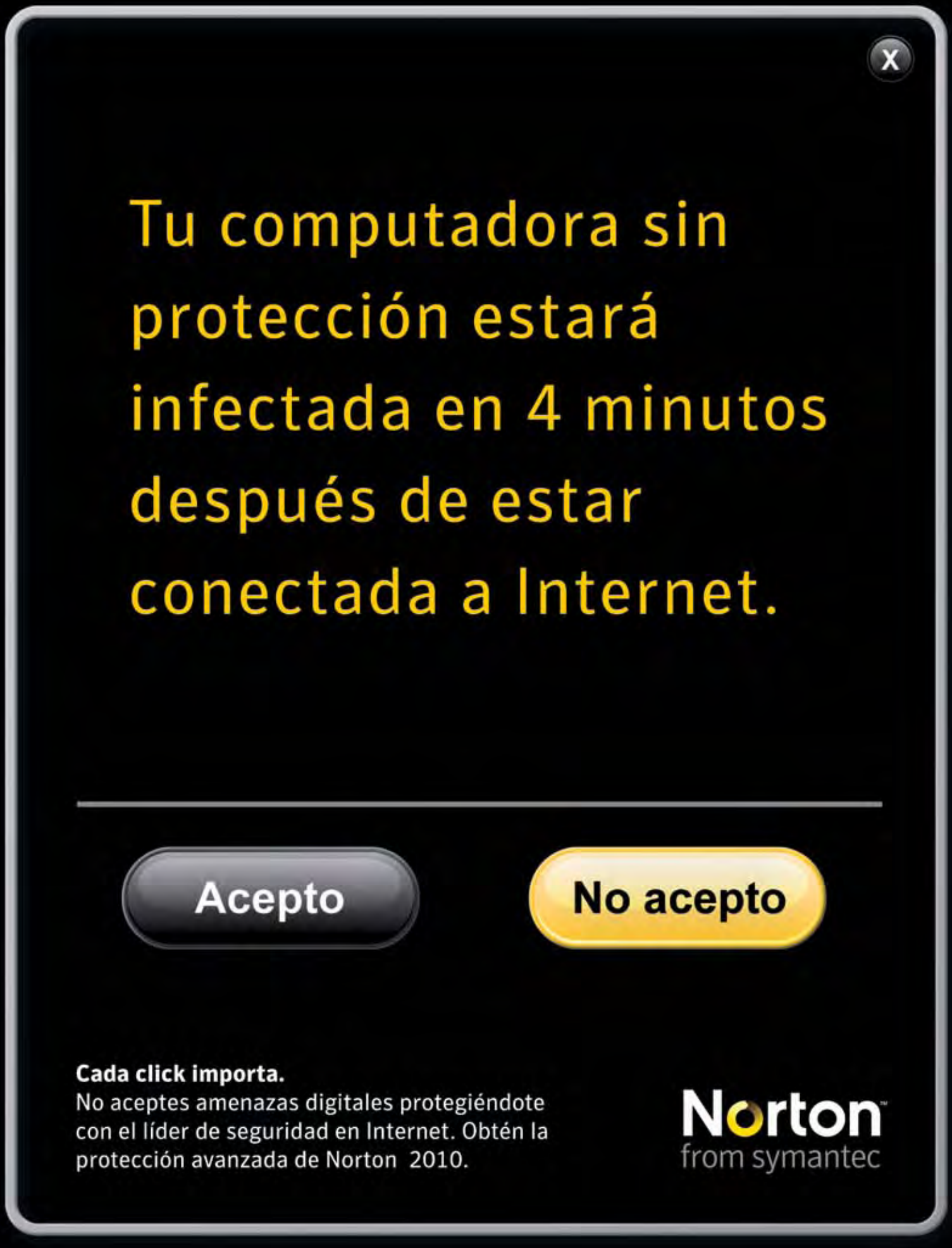
Si sus hijos adolescentes acceden a sus perfiles y a blogs desde sus teléfonos móviles, dígales que cuando lo hagan tengan buen juicio.

► Familiarícese con el "mapeo" social.

Ahora, muchos teléfonos móviles vienen con tecnología GPS instalada: los chicos que tienen este tipo de teléfono pueden determinar con precisión dónde están sus amigos—y pueden ser localizados por sus amigos. Aconséjeles a sus hijos que usen estas funciones solamente con los amigos que conocen personalmente y en quienes confían, y explíqueles por qué no es bueno que difundan su ubicación a todo el mundo durante las 24 horas del día todos los días de la semana. Además, hay algunos proveedores que ofrecen servicios GPS para que los padres puedan determinar dónde se encuentran sus hijos.

► Sea inteligente con los teléfonos inteligentes.

Muchos teléfonos incluyen acceso a internet. Si sus hi-


Tu computadora sin protección estará infectada en 4 minutos después de estar conectada a Internet.
Acepto
No acepto
Cada click importa.
No aceptes amenazas digitales protegiéndote con el líder de seguridad en Internet. Obtén la protección avanzada de Norton 2010.
Norton
from symantec

jos van a usar uno de estos teléfonos y a usted le preocupa qué es lo que pueden encontrar en la red, desactive el acceso a la red o active la función de filtro.

▶ Establezca reglas para el uso del teléfono celular.

Hable con sus hijos sobre cuándo y cómo se debe usar el teléfono celular. También puede establecer reglas para su uso responsable. ¿Les permite recibir llamadas o intercambiar mensajes de texto a la hora de la cena? ¿Estableció reglas para usar el celular en la noche? ¿Deberían entregarle los teléfonos celulares mientras que hacen la tarea escolar para no distraerse, o cuando se supone que deberían estar durmiendo?

▶ Dé el ejemplo.

Tener más aplicaciones en el teléfono móvil significa tener más elementos de distracción. En muchos estados es ilegal conducir mientras se envían o reciben mensajes de texto, mientras se navega la red o se habla por teléfono, pero hacerlo es peligroso en todos y cada uno de los estados. Dé el ejemplo y hable con sus hijos sobre el peligro que implica conducir distraído.

▶ TEXTING

Probablemente, cualquier chico que tenga un teléfono celular lo use para enviar y recibir mensajes de texto e imágenes. Esto es similar al uso del e-mail o IM, y por lo tanto también se aplican la mayoría de las reglas de buena educación y seguridad. Si sus hijos intercambian mensajes de texto, aliéntelos a:

- **Respetar a los demás. Los textos abreviados pueden causar malentendidos. Antes de mandar un mensaje de texto hay que pensar cómo puede leerlo e interpretarlo quien lo reciba.**
- **Ignorar los mensajes de texto enviados por desconocidos**
- **Aprender a bloquear números en su teléfono celular.**
- **Evitar la difusión de su número de teléfono celular en línea.**
- **No dar nunca información financiera en respuesta a un mensaje de texto.**

Proteja sus computadoras

▶ La seguridad de su computadora puede afectar su experiencia en línea—y también la de sus hijos.

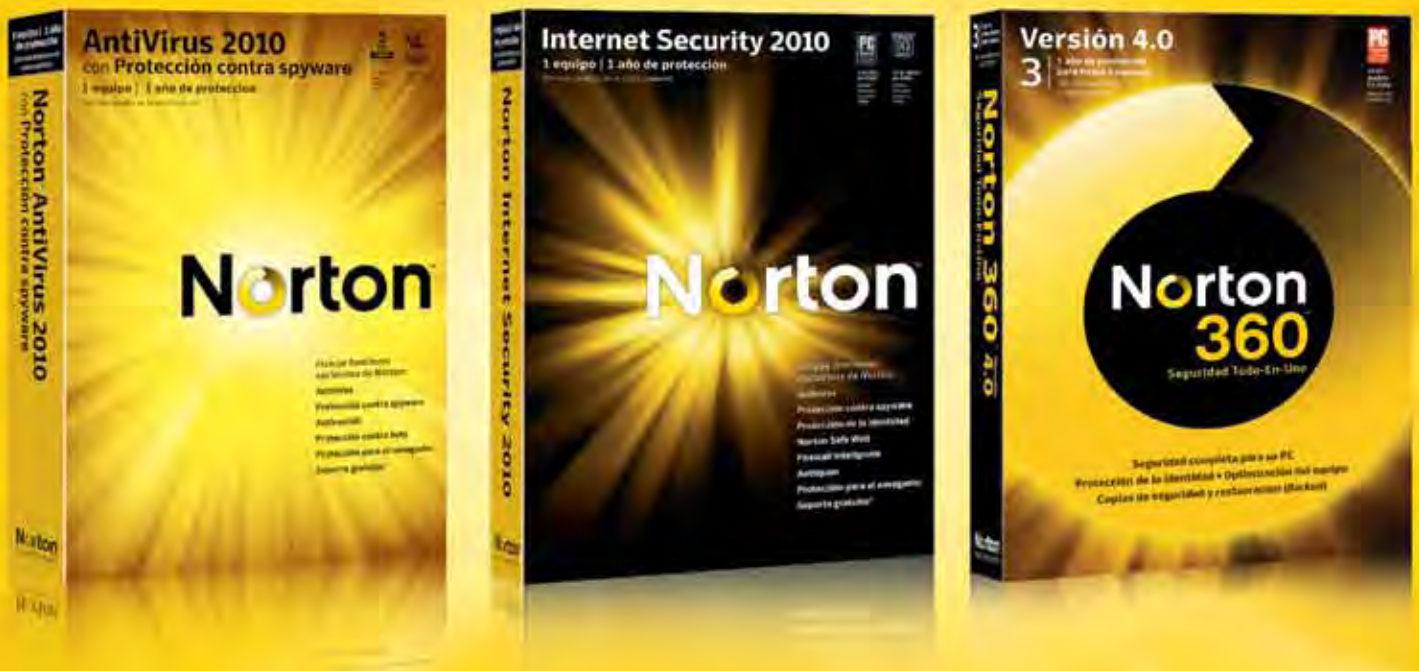
El malware (código malicioso) es un software que monitorea o controla el uso de su computadora, puede instalar virus, o puede ser utilizado para enviar anuncios de aparición automática indeseados, redirigir su computadora a sitios Web que no desea visitar, o para grabar lo que escribe en su teclado. Si le instalan inadvertidamente un malware en su computadora, otra persona podría robarle la información personal de su familia.

¿QUÉ PUEDE HACER USTED?

▶ Use un software de seguridad y actualícelo regularmente.

Los programas antivirus y anti-spyware escanean las comunicaciones entrantes para detectar los archivos problemáticos; el firewall bloquea las comunicaciones provenientes de fuentes no autorizadas. Busque programas con capacidad de revertir el daño y que se actualicen automáticamente.

No aceptes amenazas digitales,
protégete con Norton™.



Descarga una prueba gratis por 30 días de:

Norton 360™ Versión 4.0 en:
www.norton.com.mx/pruebeN360

Norton™ Internet Security 2010 en:
www.norton.com.mx/pruebeNIS2010

Cada click importa.

Norton™
from symantec

► Mantenga actualizados su sistema operativo y navegador de internet e infórmese sobre las funciones de seguridad.

Los hackers o piratas informáticos se aprovechan de los programas del sistema operativo y navegadores que no tienen instaladas las actualizaciones de seguridad más recientes. Aumente el nivel de seguridad de su computadora cambiando la configuración de seguridad y privacidad del sistema operativo o navegador de su computadora. Para aprender a cambiar la configuración predeterminada de fábrica, consulte el menú de "Herramientas" (Tools) u "Opciones" (Options).

► Tenga cuidado con las cosas "gratis."

Los juegos, timbres de teléfono u otras descargas pueden esconder un programa malicioso o malware. Dígales a sus hijos que no descarguen nada a menos que confíen en la fuente y que lo hayan escaneado con el programa de seguridad.

► P2P-ARCHIVOS COMPARTIDOS (redes Punto a Punto)

Algunos chicos comparten música, juegos o programas en línea. El P2P o uso compartido de archivos es un sistema que permite que las personas compartan este tipo de archivos a través de una red informal de computadoras que utilizan el mismo programa. Si sus hijos descargan material protegido por la legislación de derecho de autor, usted podría verse involucrado en problemas legales. A veces, un archivo compartido puede tener escondido un programa espía, malware o material pornográfico. Le damos algunas recomendaciones para ayudar a sus hijos a compartir archivos sin riesgos:

Instale el software de archivos compartidos correctamente. Active las características predeterminadas correctas para no compartir ninguno de los datos privados. Casi todas las aplicaciones de archivos compartidos o P2P vienen predeterminadas para compartir los archivos descargados en su archivo de "guardar" o "descargar". Por esta razón, es importante configurar el programa para que no lo haga.

Si usted no configura correctamente estas funciones, los demás usuarios de P2P pueden acceder a los archivos que usted no desea compartir, incluso a los documentos personales archivados en el disco duro de su computadora, como por ejemplo sus declaraciones de impuestos u otros documentos financieros.

Antes de que sus hijos abran o ejecuten un archivo descargado, dígales que lo escaneen con el programa de seguridad. Asegúrese de que el programa de seguridad esté actualizado y en funcionamiento mientras que la computadora está conectada a internet.

Controles paternos

Si le preocupa lo que sus hijos pueden llegar a ver mientras navegan por internet—especialmente si tiene hijos en edad de escuela primaria— puede tomar en consideración algunas herramientas. Tenga presente que si bien los controles paternos pueden funcionar bien para los pequeños, los adolescentes que llevan años de experiencia en línea podrán desactivarlos o esquivarlos fácilmente o encontrar otras computadoras para acceder a los sitios que desean visitar.

► La mejor manera de proteger a sus hijos mientras están en línea es hablar con ellos.

Cuando los niños quieren información importante, mayormente cuentan con sus padres. Los niños valoran las opiniones de otros niños. Pero tienden a confiar en sus

padres para ayuda en los asuntos de mayor importancia.

Algunas opciones que los padres de familia pueden explorar para cuidar la navegación de los niños más pequeños son:

▶ Filtro y bloqueo.

Estas herramientas limitan el acceso a ciertos sitios, palabras o imágenes. Hay algunos productos que establecen por sí mismos qué material filtrar y hay otros que permiten que los padres establezcan los filtros. Algunos filtros se aplican a los sitios Web y hay otros que sirven para el e-mail, chat y mensajes instantáneos.

▶ Bloqueo de contenido saliente.

Este software impide que los chicos compartan información personal en línea, en salas de chateo o vía e-mail.

▶ Límite de tiempo.

Este programa le permite limitar la cantidad de tiempo que sus hijos pasan en línea y establece la hora del día en que pueden acceder a internet.

▶ Navegadores para niños.

Estos navegadores filtran palabras o imágenes

no aptas para el público infantil. Lamentablemente existe poca disponibilidad de versiones en español.

▶ Motores de búsqueda para niños.

Estos motores hacen búsquedas limitadas o evalúan los resultados de la búsqueda de sitios y material apto para niños. Al igual que en el caso anterior, lamentablemente existe poca disponibilidad de versiones en español.

▶ Herramientas de monitoreo.

Este software alerta a los padres sobre la actividad desarrollada en línea sin bloquear el acceso. Hay algunas herramientas que registran el domicilio de los sitios Web visitados por un chico; y hay otras que envían un mensaje de advertencia cuando se visitan determinados sitios. Las herramientas de monitoreo pueden utilizarse con o sin el conocimiento del niño.

Proteja la privacidad de sus hijos preadolecentes

▶ Muchos sitios que sus hijos visitan pueden solicitar información sobre ellos, frecuentemente de forma lícita.

La información personal de su hijo es valiosa, y usted puede hacer muchas cosas para protegerla:

▶ Sea selectivo con su permiso.

Los sitios pueden solicitarle su autorización por varios medios, entre los que se incluyen el correo electrónico o postal. Antes de dar su consentimiento asegúrese de saber qué información desea recolectar el sitio y qué es lo que prevé hacer con ella. También considere qué grado de autorización está dispuesto a conceder —en muchos casos no se trata de dar permiso para todo o nada. Posiblemente pueda dar autorización a la compañía para que recolecten algunos datos personales de su hijo, pero sin permitir que la compartan con terceros.

▶ Sepa cuáles son sus derechos.

Como padre, usted tiene derecho a ver cualquier tipo de información personal que un sitio haya recolectado sobre su hijo. Si usted solicita ver la información, los operadores del sitio Web necesitarán comprobar que usted es realmente el padre o madre o pueden optar por eliminar la información. Usted también tiene derecho a revocar su autorización y exigir que eliminen la información sobre su hijo.

▶ Controle los sitios Web que sus hijos visitan.

Si se trata de un sitio Web en el que los usuarios deben registrarse, vea qué tipo de información solicitan para hacerlo y evalúe si está o no de acuerdo con los datos que solicitan. También puede controlar si el sitio parece cumplir con las reglas más básicas, como por ejemplo exhibir la política de privacidad para padres de manera clara y destacada.

▶ Lea la política de privacidad.

El sólo hecho de que un sitio tenga una política de privacidad no necesariamente significa que proteja la privacidad de la información personal. La política de privacidad puede ayudarlo a deducir si está de acuerdo con la información que recolecta el sitio y cómo prevé usar o compartir esa información. Si la política de privacidad dice que no limita la cantidad o tipo de datos que recolecta, o que no ejerce control sobre las personas que pueden acceder al sitio, significa que no hay límites.

▶ Haga preguntas.

Si no entiende las prácticas o normas de un sitio Web, pida explicaciones. La política de privacidad debería incluir la información de contacto de una persona preparada para responder a sus preguntas.

▶ Denuncie a los sitios Web que no cumplan las reglas.

Si cree que un sitio Web ha recolectado o divulgado información sobre sus hijos o que ha comercializado los datos de una manera contraria a la ley, presente una denuncia en: **www.asi-mexico.org/denuncia.**

Copyright: www.alertaenlinea.gov
Agradecemos al portal propiedad de FTC en los Estados Unidos habernos permitido tomar partes de su guía NETCETERA © para esta publicación.

el rol de la escuela

Para todos es evidente la importancia histórica de las escuelas en el desarrollo de las sociedades.

La educación que imparten ha provisto a la humanidad en todas sus épocas, de la formación dirigida a la adquisición de conocimientos o al desarrollo intelectual, social, moral, cívico, ético, de costumbres y de formas de actuar de muchas generaciones..

Hoy en día, las escuelas no escapan del reto que significa entender la forma en que las nuevas Tecnologías de Información y Comunicación (TICs) están impactando a la sociedad, principalmente entre los niños y niñas que asisten a los planteles, y que utilizan Internet y los celulares como su medio predilecto de comunicación, entretenimiento y acceso a información. Ellos aprovechan los dispositivos digitales a su disposición para vincularse con otros, sostener y fortalecer sus relaciones sociales, desarrollar comunidades de intereses comunes, e incluso, se han convertido en creadores de contenido multimedia que comparten abiertamente con otros usuarios.

- **¿Qué pueden hacer las escuelas?**
- **Programa cíclico de 7 pasos en períodos anuales**
- **Entrevista a Kenneth Peterson, director general de los Colegios Peterson**

¿Qué pueden hacer las escuelas?

El desafío para las escuelas consiste en poder guiarlos para aprovechar al máximo el poder de estas tecnologías, en forma segura y responsable, aprendiendo a distinguir entre información valiosa y aquella en la que no pueden confiar, enseñando normas y conductas adecuadas que les ayuden a identificar y evitar situaciones que puedan poner en riesgo su integridad, tanto física como emocional.

Es necesario entonces que las escuelas impulsen en niños, niñas y adolescentes el desarrollo del CRITERIO que les permita desenvolverse apropiadamente dentro de este nuevo paradigma de comunicación, socialización y entretenimiento digital, fortaleciendo las competencias básicas que les permitan además, replicar estas capacidades favorablemente en su propio entorno familiar.

▶ EL DESARROLLO DE ESTAS COMPETENCIAS BÁSICAS, COMO:

- Manejo de la privacidad en Internet
- Identificación de áreas de riesgo
- Democratización del conocimiento
- Construcción de relaciones no presenciales, etc…

Son objetivos cubiertos por el programa CENETIC Escolar (Centro de Evaluación de Tecnologías de Información y Comunicación) de nuestra asociación civil, que ofrece a las escuelas material educativo para la enseñanza de:

- **CIBER-CIUDADANÍA.**
  Deberes y derechos de los usuarios de internet
- **ALFABETIZACIÓN DIGITAL.**
  Criterio para uso de los medios a sus disposición

Es un programa cíclico que inicia con la generación de métricas sobre Hábitos, exposición a riesgos y manejo de privacidad en Internet. Con esta valiosa información como punto de partida, ofrecemos una conferencia a la comunidad escolar, entregamos un reglamento de uso de tecnología en el plantel, ofrecemos guías de mejores prácticas en el uso de Internet y Celulares dirigidas a Padres de Familia, y capacitamos a profesores con guías de docentes en los temas de Ciber-ciudadanía y Alfabetización digital.

Favor de solicitar información adicional o presentaciones en el correo: contacto@asi-mexico.org

Entrevista a Kenneth Peterson, director general de los Colegios Peterson

Hoy vamos a platicar sobre seguridad de los menores de edad en internet, y el impacto, positivo o negativo que el uso de tecnologías de información y comunicación ha tenido en los estudiantes de las nuevas generaciones.

¿Ha disminuido el aprovechamiento escolar en estas generaciones? (Por usar tanto internet por las tardes) Háblanos del impacto en términos generales.

Aunque si se ha visto una disminución en los resultados escolares de estas generaciones no solo en México, si no que a nivel internacional, difícilmente es atribuible únicamente a internet. Inclusive, hay aspectos muy positivos del uso de la computadora y del internet que son muy alentadores. Por ejemplo, se está substituyendo horas de televisión, que es una actividad meramente pasiva, por horas de actividades interactivas con la computadora. Esto crea un ambiente de más riqueza y mayor estimulación para ellos. Otro gran beneficio es el acceso a una cantidad de materiales, información, juegos interactivos y recursos didácticos que difícilmente hubieran tenido acceso generaciones anteriores.

La encuesta A.S.I. de marzo del 2010 encontró que en opinión del 82% de los encuestados señala que el concepto de "Seguridad en internet" debería enseñarse en forma obligatoria en las escuelas. ¿Cuál es tu opinión?

Yo estoy de acuerdo que debería ser obligatorio, ya que la seguridad de nuestros alumnos tiene que ser una primera prioridad. La alternativa es perder la gran riqueza de lo que ofrece el internet por los riesgos potenciales a los que se pueden enfrentar los alumnos en su uso. Por lo tanto, es mejor fomentar su uso de una forma responsable, preparando a los alumnos de antemano con estas medidas preventivas. En los Colegios Peterson, cursos de seguridad forma parte de la capacitación de nuestros alumnos.

¿Qué problemas ves en el futuro inmediato en caso de no incorporar esta educación en los planteles?

Que un número pequeño de incidentes graves resulten en medidas que limiten o prohíban el uso del internet para los alumnos, con la pérdida para ellos de los grandes beneficios que si ofrece.

¿Cómo se puede medir el beneficio de educar a los niños en este tema?

Con parámetros específicos, como el número de casos reportados por parte de los alumnos de contactos inadecuados a los que se han enfrentado (en vez de que se los callan). También a través de encuestas periódicas, donde se les debe de preguntar si han tenido contactos inapropiados o si han sido expuestos a material inadecuado, y cuál ha sido su respuesta. Por ejemplo, si lo han reportado a algún adulto, como sus padres o maestros. La esperanza es que el porcentaje de alumnos dispuestos a reportar este tipo de incidentes aumente con la educación sobre seguridad en internet.

Frecuentemente se dice que los niños de esta generación nacieron con "el chip puesto", y que son capaces de hacer múltiples cosas en forma simultánea, mientras que autoridades médicas confirman que el cerebro humano no puede trabajar así, y que por lo tanto el aprovechamiento académico se ve disminuido. ¿Cuál es tu pronóstico sobre el nivel de preparación que tendrán estos menores cuando inicie su etapa laboral?

Estos alumnos se estarán enfrentando a un mundo de trabajo radicalmente diferente al de hoy en día, con un alto componente del uso de tecnología. Nuestra responsabilidad es prepararlos para tener éxito dentro de la misma. Los Colegios Peterson preparan a sus alumnos con las competencias de un colegio del siglo XXI, incluyendo el manejo de proyectos, habilidades de comunicación y trabajo en equipo.

En los EUA hay muchas escuelas que están aprovechando la tecnología iTouch para que los alumnos interactúen con el profesor, por ejemplo para responder pruebas rápidas por medio de tecnología inalámbrica, pero en

45 Años
Innovando la educación en México

PETERSON HIGH SCHOOLS

CAMPUS TLALPAN **CAMPUS CUAJIMALPA**

- 45 años como líder en la educación en México.
- Programa educacional de excelencia tipo estadounidense.
- Alto nivel en inglés.
- Profesorado altamente calificado.
- Ambiente saludable y libre de drogas.
- Profundo programa de valores.
- Nuestros egresados asisten a las mejores universidades en Mexico, EUA y el resto del mundo.
- Ambiente multicultural.
- Becas por mérito.

Tres Certificaciones
EUA, México
Bachillerato Internacional

SEP

ISAS Independent Schools Association of the Southwest

ib

www.peterson.edu.mx

CAMPUS TLALPAN

Admisiones: Ceci Barrientos
Tel.: 5849-1885
e-mail: cecibarrientos@peterson.edu.mx

CAMPUS CUAJIMALPA

Admisiones: Karina Galvan
Tels. 5813-0114, 5813-0116
e-mail: karina_galvan@peterson.edu.mx

México vemos que en muchos planteles incluso se prohíbe su uso en clases. ¿Cuál es el equilibrio adecuado, o consideras que se debe limitar el uso de tecnología en la escuela?

Mi opinión es que la tecnología iTouch puede ser un complemento positivo dentro del salón de clase, pero hay que capacitar a los profesores en su uso antes de introducirlo. Como toda tecnología, ofrece beneficios pero también retos y peligros, y sabiendo cómo usarlo se puede buscar sacarle el máximo potencial a esta herramienta y limitar los aspectos negativos.

¿Cómo sientes la preparación de los profesores para canalizar adecuadamente la energía de los menores de edad hacia las nuevas tecnologías Y en su caso, ¿Qué deben hacer para mantener el ritmo del avance tecnológico?

Los menores van a buscar y usar estas nuevas tecnologías, con o sin el respaldo de los profesores. Nuestro reto como educadores es prepararlos y guiarlos para que este uso sea constructivo y de beneficio para ellos, y no solo como algo que sea un distractor o puro entretenimiento.

¿Qué hace tu escuela para desarrollar nuevas habilidades y competencias digitales entre los alumnos del plantel?

Se les capacita en el uso de las tecnologías de información, de las herramientas específicas que tiene el Colegio contratado, incluyendo recursos en línea tales como EBSCO, United Streaming, Discovery, y otros. Se les proporciona información acerca de sus actividades, tareas y demás trabajos académicos a través de medios digitales incluyendo nuestro portal para alumnos. Esto incluye el acceso no solo a las tareas solicitadas, sino también a las rúbricas sobre la cual van a ser evaluados. Por supuesto, se fomenta la comunicación con sus profesores a través de medios electrónicos como respaldo a sus actividades de aprendizaje.

¿Consideras que con una buena educación en ciber-ciudadanía, y con desarrollo de habilidades y competencias digitales entre los niños, los problemas como el Hostigamiento en Línea (Cyber-bullying) y la Difamación disminuirían?

Mi opinión es que con una buena educación en ciber-ciudadanía, forzosamente tendrá que disminuir este tipo de problemas ya que esto tendrá que crear conciencia entre los jóvenes del impacto negativo que pueden ocasionar este tipo de comportamientos. Creará sensibilidad hacia el tema y esto tiende a limitar los incidentes de los comportamientos negativos. En el Peterson, nuestra meta es ser el colegio más sano de México. Por lo tanto, hacemos un énfasis especial en habilidades de manejo de emociones y la prevención de todo tipo de bullying.

Finalmente, mucho se habla del bajo nivel de involucramiento de los padres de familia en las actividades de sus propios hijos en internet, en tu experiencia, ¿Cómo se puede lograr una participación más activa de su parte, y que piensas que puede hacer la escuela para lograrlo?

Es vital la involucración de los padres en todos los aspectos de la educación de sus hijos, y en particular en un tema tan delicado como el uso del internet. Por lo tanto, la escuela y el hogar deberán hacer mancuerna para poder apoyar de forma conjunta a sus hijos y ser consistente en la aplicación de reglas del uso de estas tecnologías. De poco sirve tener filtros y maestros pendientes en el colegio, si al llegar a la casa tienen su propia computadora en su cuarto y no cuentan con ninguna supervisión. En el Peterson, trabajamos de cerca con nuestra comunidad a través de nuestra escuela de padres para respaldar este trabajo en equipo.

¡Muchas gracias!

Alianza por la Seguridad en Internet A.C.

internet productivo

En esta sección, presentaremos servicios en la red que permiten elevar la productividad del usuario, de su familia o incluso de su empresa, principalmente en las áreas de Banca, Comercio y Gobierno electrónicos.

Beneficios de la banca en línea

La Banca en Línea, que llego para quedarse con Internet, es posiblemente uno de los servicios que mayor impacto positivo ofrece a los usuarios mexicanos, elevando su productividad, ahorrando tiempo y dinero, y ofreciendo total conveniencia tanto a los bancos como a sus clientes, por su flexibilidad de horarios, variedad de servicios, mejores comisiones, etc…

Hay una gran cantidad de servicios que la Banca Mexicana pone a disposición de los usuarios de Internet en forma segura y conveniente, resaltando:

- **CONSULTA DE SALDOS Y ESTADOS DE CUENTA.**
- **ADMINISTRACIÓN DE INVERSIONES**
- **PAGAR SERVICIOS COMO LUZ, TELÉFONO, IMPUESTOS, ETC. , CON OPCIONES AUTOMATIZABLES.**
- **PAGOS A PROVEEDORES NACIONALES Y EXTRANJEROS**
- **TRASPASOS DE FONDOS ENTRE CUENTAS PROPIAS Y DE TERCEROS.**
- **PAGOS AUTOMÁTICOS DE NÓMINAS.**
- **PAGAR TARJETAS DE CRÉDITO, Y MUCHOS MÁS.**

Los usuarios de la banca en línea disfrutan de muchos beneficios, sobre todo en áreas metropolitanas donde el traslado físico del cliente a la sucursal consume mucho tiempo, y existen mayores riesgos al portar dinero en efectivo. Hay múltiples beneficios adicionales:

- **RAPIDEZ Y FACILIDAD EN LAS OPERACIONES.**
- **EVITAR COMISIONES AL PAGAR SERVICIOS EN VENTANILLAS BANCARIAS.**
- **PAGOS PROGRAMADOS CON ANTICIPACIÓN**
- **MONITOREO PERMANENTE DE SALDOS PARA CONFIRMACIÓN DE DEPÓSITOS EVITANDO SOBREGIROS**
- **CONVENIENCIA DE HORARIOS, HAY BANCOS CUYOS SERVICIOS ESTÁN DISPONIBLES LAS 24 HORAS DEL DÍA, LOS 365 DÍAS DEL AÑO**

Si bien Internet es una tecnología que ofrece seguridad y confidencialidad para el proceso de transacciones bancarias, es importante que el usuario la utilice cuidando algunos aspectos que le garanticen experiencias positivas y aproveche al máximo esta poderosa tecnología, es por ello que en A.S.I. hemos preparado esta guía de recomendaciones y Mejores Prácticas que esperamos sean de mucha utilidad.

1. CONOCE LOS SERVICIOS DE SEGURIDAD DEL PORTAL DE TU BANCO.

Acércate a tu ejecutivo de cuenta para que te explique las diferentes medidas de seguridad de su portal, las señales que debes aprender a distinguir, y las alertas a tu disposición para asegurarte un uso seguro y productivo de la tecnología en tu favor. ¿Sabías por ejemplo que puedes recibir un mensaje directamente en tu teléfono celular cada vez que se efectúa un movimiento en tu cuenta?

2. INGRESA DIRECTAMENTE AL PORTAL DE TU BANCO

No es recomendable seguir ligas en otros sitios o en

correos electrónicos para visitar el sitio de tu banco, ya que de esta forma puedes ser engañado y llevado a un sitio falso. Los delincuentes disfrazan sitios fraudulentos para hacerlos parecer legítimos y solicitarte información confidencial

La forma más segura de visitar el sitio de tu banco es escribir su dirección directamente en tu navegador, por ejemplo:

3. VERIFICA LAS SEÑALES BASICAS DE SEGURIDAD.

Cerciórate de que el sitio en el que ingresarás para realizar tus operaciones bancarias utiliza tecnología segura. La dirección del navegador debe comenzar con https: , donde la ‘ s ‘ significa ‘Seguro’.

Es muy importante resaltar que el portal principal de tu banco puede especificar inicialmente la dirección con el indicador http:, ya que en esa página no se realizan transacciones, es solo la página en la que se muestran datos generales, información financiera de propósito informativo, etc…, pero una vez que ingresas con tu nombre de usuario y contraseña a la sección transaccional del sitio, debes encontrar el indicador https: que te indica que la información que ingreses estará segura, por ejemplo:

También es importante localizar el ícono del candado en la barra de estado.

Desgraciadamente ningún elemento es seguro a ‘prueba de balas’, pero estos indicadores permiten eliminar prácticamente por completo la posibilidad de que seas víctima de algún fraude, y acompañado del resto de los consejos de esta sección, dicha posibilidad es casi nula.

4. CUIDA TU IDENTIDAD ELECTRÓNICA.

Casi todos los esquemas de seguridad establecen que una persona requiere cuando menos de un Nombre de Usuario y una Contraseña para tener acceso a áreas o servicios privados, como son su Correo electrónico, sus Cuentas de Banco, sus Tarjetas de Crédito o bien, su propia computadora.

Estos elementos, como son Nombre de Usuario, Contraseñas, Tarjetas de Códigos, y demás dispositivos de seguridad forman lo que se conoce como ‘ Identidad Electrónica ó Identidad Digital ‘, o en algunos medios se denomina ‘Credenciales’ de un usuario, y son las que le permiten acceder a información y sitios restringidos.

Debes tener especial cuidado en no divulgar tu identidad electrónica a nadie. Si una persona llega a disponer de tu Identidad Electrónica, puede con ella entrar a tus cuentas, ver tus saldos, ordenar traspasos, comprar productos, y hacer todo lo que tú mismo harías sin que la institución financiera tenga forma de saber que no eres precisamente tú el que las está haciendo.

Tampoco es recomendable almacenar la información de tu Identidad Electrónica en archivos localizados en tu propia computadora, o al alcance de otros usuarios de la misma o de la red en la que se encuentre tu equipo.

5. UTILIZA CONTRASEÑAS SEGURAS.

Una contraseña debe tener cuatro características básicas para considerarse segura:

1. Debe ser **SÓLIDA.**
   Utilizar combinaciones de Mayúsculas/Minúsculas, Números, y si el sitio lo permite, símbolos.

2. Debe ser **ÚNICA.**
   La contraseña que uses para operaciones financieras no debe estar relacionada con cualquiera de tus otras contraseñas. Conviene que cada contraseña que utilices sea al menos ligeramente diferente de las demás, especiamente si se trata de la que usas para entrar a tu banco.

6. EVITA REALIZAR OPERACIONES BANCARIAS EN SITIOS PÚBLICOS

Las computadoras en sitios públicos como Cafés Internet y Aeropuertos son fácil blanco de personas malintencionadas que siembran en ellas código malicioso capaz de registrar todo lo que escribas en el teclado, por lo que sería muy fácil apoderarse de tus datos confidenciales, por lo que no es recomendable utilizar estos lugares para realizar operaciones financieras.

Evita también hacer operaciones en redes inalámbricas no seguras. Si tu casa u oficina cuenta con este tipo de red, cerciórate de que tu información viaje protegida por una contraseña. (encriptada), Recuerda que hoy en día es común que una red inalámbrica pueda ser accedida desde distancias incluso mayores a 100 metros.

Si utilizas este tipo de accesos a Internet por alguna urgencia, te sugerimos cambiar tus contraseñas lo más pronto posible, y se especialmente precavido al realizarlas.

7. TEN CUIDADO CON CORREOS ELECTRÓNICOS FRAUDULENTOS.

Debes contar con que tu banco NUNCA te solicitará datos confidenciales, ni por teléfono ni mucho menos por correo electrónico. Esto incluye contraseñas, números de cuenta, llaves de OTP, claves de acceso, NIPs, etc…

Los correos electrónicos que te solicitan este tipo de información son fraudulentos y debes desconfiar siempre de ellos y reportarlos a tu banco. Igualmente debes evitar aquellos correos que te invitan a visitar otras páginas en donde también te pedirán información sensible.

Esta modalidad de engaños se conoce como Phishing, si recibes un correo de este tipo debes reportarlo de inmediato a tu banco.

3. Debe ser **PRÁCTICA.**
¿Podrías recordarla sin tener que escribirla? Además, no debe existir en ningún diccionario, incluso en otros idiomas.

4. Debe ser **RECIENTE.**
Cámbiala con cierta frecuencia, se recomienda cada 60 ó 90 días. Esta es una práctica muy recomendable por si acaso llega a caer en manos indebidas.

Nunca sigas ligas o vínculos (links) ni descargues archivos adjuntos en correos de personas desconocidas, pues podrían ser un virus o programas que intentarán robar tu información.

8. APLICA REGLAS DE SEGURIDAD BÁSICA PARA TU EQUIPO.

Tu equipo debe estar libre de virus y códigos maliciosos como el spyware, que son capaces de registrar lo que haces y enviarlo después a sitios fraudulentos. Haz especial hincapié en mantener limpio el equipo con el que realizas operaciones bancarias para evitar ser víctima de un fraude.

No olvides activar la función de 'Actualizaciones Automáticas' para tu sistema operativo, de forma que siempre esté al día con las actualizaciones de seguridad disponibles.

Finalmente, para evitar que usuarios malintencionados accedan a tu computadora, utiliza un Firewall.

Hoy en día hay muchas aplicaciones comerciales que reúnen y exceden estos requisitos, ofreciéndote máxima protección.

9. NO INSTALES SOFTWARE PIRATA.

Es muy común que el software ilegal contenga virus y otros tipos de códigos maliciosos que podrían dañar tu equipo o peor aún, obtener tu información confidencial.

10. CIERRA TU SESIÓN CUANDO TERMINES TUS OPERACIONES.

Siempre que termines tus operaciones bancarias, haz clic en el botón 'Cerrar Sesión' o 'Salir'.

Es muy recomendable que también cierres la ventana del explorador que utilizaste para hacer tus operaciones, y no permitas que nadie te observe mientras trabajas, principalmente cuando digitas tus claves de acceso o cualquier otra información sensible.

Y FINALMENTE, SÉ PRECAVIDO.

Si algo no te parece normal o razonable al visitar el portal de tu banco, consulta de inmediato con tu ejecutivo de cuenta antes de efectuar cualquier operación, La Precaución es el mejor aliado para aprovechar la tecnología de forma tranquila.

Es mejor partir de no creer nada y después averiguar, que viceversa.

internet Bibliográfico

Expertos del ramo le presentan en esta sección recomendaciones de libros que le permitirán conocer Internet desde diferentes y siempre interesantes puntos de vista.

En esta edición recomendamos

▶ ETHICAL HACKING. UN ENFOQUE METODOLÓGICO PARA PROFESIONALES.

Ezequiel Sallis, Claudio Caracciolo y Marcelo Rodriguez
Págs. 135
Alfaomega Grupo Editor © 2010

Este libro es una propuesta diferente que le permitirá comprender los aspectos metodológicos asociados a un Ethical Hacking (Intrusiones éticas) y los diferentes tipos de análisis de seguridad existentes. El libro va más allá de las herramientas utilizadas, para enfocarse sobre los objetos asociados a cada etapa de un análisis de seguridad, permitiéndose de esta forma ser un material de consulta que perdurará en el tiempo.

Escrito de manera sencilla, con sentido común y bajo la experiencia de los autores, los lectores conocerán las técnicas de identificación y explotación de vulnerabilidades más utilizadas en la actualidad.

▶ CÓMO SOBREVIVIR EN LA RED.

David Rodriguez de Sepúlveda Maillo y Sixto Rodriguez de Sepúlveda Maillo.
Págs. 189
Alfaomega /RA-MA © 2010

Un libro que no puede faltar en la biblioteca familiar, ya que además de cubrir aspectos teóricos en relación a los factores que más pueden afectar el uso de Internet, es un libro eminentemente práctico orientado a la gran mayoría de los recursos que existen en la red como correo electrónico, blogs, podcasts, wikis y redes sociales.

Es una excelente opción para padres de familia, profesores y alumnos que utilizan Internet, porque así como es una herramienta muy buena y un excelente medio de comunicación, también existen riesgos que debemos conocer para evitarlos.

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

LÍNEA DE DENUNCIA
Reporte de contenido ilegal, inapropiado y fraudulento

LOS MÁS REPORTADOS
Acceso a información de sitios reportados por la comunidad

SITIOS RECOMENDADOS PARA MENORES
Relación de sitios avalados para acceso de menores de edad

CENETIC
Repositorio de encuestas on-line respondidas en el sitio

REPOSITORIO DE CONTENIDOS
Compendio de contenidos educaticos y de orientación creados a partir de las denuncias recibidas

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

CONFERENCIAS
Sesiones sobre uso seguro y responsable de internet

VIDEOS EDUCATIVOS
Selección de videos de información y prevención sobre seguridad en internet, principalmente para menores de edad

MATERIAL PARA ESCUELAS
Encuestas y materiales de apoyo para el sistema educativo

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

CORRE LA VOZ
Materiales para publicar la línea de denuncia en sitios independientes

FAQ
Recopilación de preguntas relevantes en las categorías de General, Técnicas, Malware y jurídica

NOTICIAS
Compendio de noticias relevantes sobre seguridad en internet

CONTACTO
Centro de recepción de comentarios, sugerencias y preguntas de los visitantes del sitio

Cuida tu mundo
Navegación Segura
La conexión más rápida en
infinitum®
El servicio de navegación segura es gratis para clientes infinitum.
descárgalo en telmex.com
01 800 123 2222
Tiendas TELMEX telmex.com
TELMEX®
está contigo