EL EFECTO INTERNET

www.asi-mexico.org

DELITOS CIBERNÉTICOS:

- ✓ CONÓCELOS
- ✓ EVÍTALOS
- ✓ DENÚNCIALOS

Alianza por la SEGURIDAD en Internet

Internet alternativo

Internet en tu familia

Año 1. Número 1 .

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 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

Señores,

Su revista me parece muy necesaria para los papás que no conocemos bien las computadoras, pero que sí nos interesa al menos saber qué hacen nuestros hijos. Una cosa que he escuchado mucho es que deben usar contraseñas muy buenas para proteger nuestra identidad, sobre esto ¿podrían publicar información? Muchas gracias. *Magdalena E.*

Respuesta:
Efectivamente, la contraseña, junto con el nombre de usuario, integran hoy en día la llamada "identidad digital" de los usuarios de Internet, y existen recomendaciones muy concretas para lograr que sean lo más seguras posibles. En el ejemplar anterior dimos recomendaciones especiales para los usuarios de banca electrónica, y en el próximo ejemplar incluiremos mejores prácticas para la creación de contraseñas seguras dentro de la sección "Internet Productivo".

Envía tus comentarios a efecto@asi-mexico.org

¿Quieres colaborar?

Si tienes un artículo o contenido que pueda ser de utilidad para el usuario de Internet de México, y piensas que puede ayudar a tener mejores experiencias con la red, envíanos un correo a editorial@asi-mexico.org y con mucho gusto lo consideraremos.

Cartas al editor

Nos interesa mucho tu opinión, así como sugerencias, quejas o cualquier comentario relativo a esta publicación. Por favor, escríbenos a contacto@asi-mexico.org, te agradeceremos la oportunidad que nos das de mejorar.

EDITORIAL

Internet S.O.S.

La Alianza por la Seguridad en Internet (ASI) es responsable de la operación de la Línea Ciudadana de Denuncia de Contenido Ilegal o Fraudulento en Internet.

Muchos de los reportes recibidos en la Línea no corresponden a delitos en nuestra legislación actual, como es el caso de usuarios molestos por recibir *spam* (correo electrónico no solicitado). Para todos ellos, elaboramos contenidos de orientación, que ayuden a los usuarios a evitar estas molestias, y los ponemos a disposición del público en nuestro repositorio de contenidos, en donde se pueden consultar e incluso descargar en formato pdf para su mejor aprovechamiento.

En otros casos, usuarios son víctimas por ejemplo de fraudes menores, cometidos por páginas alojadas en el extranjero, que por su complejidad son muy difíciles de perseguir y, sobre todo, de resolver a favor de las víctimas, como es el caso del denominado "Fraude nigeriano", que se origina en diversos países de África y que busca sustraer cantidades entre 300 y 2000 pesos a las víctimas, y que para su esclarecimiento requerirían de la participación de policías internacionales, como el FBI o Interpol, que por estos montos no justifican internamente su participación.

Si bien es cierto que para el afectado cualquier monto, por mínimo que sea, es importante, la realidad es que estos casos —que suceden en decenas de miles de ocasiones diariamente— representan un volumen imposible de atender para cualquier autoridad en cualquier parte del mundo, por lo que, al igual que en el caso del *spam* antes mencionado, ponemos a disposición del usuario los más completos contenidos de orientación para la prevención de estas calamidades digitales.

Sin embargo, ha venido creciendo la cantidad de reportes de hechos que sí pueden ser constitutivos de delitos y que son turnados automáticamente a las autoridades correspondientes, razón por la cual hemos solicitado a la Unidad de Investigación Cibernética de la Procuraduría General de Justicia del Distrito Federal que nos ayude a explicarle a todos los usuarios cuáles son los delitos cibernéticos, cómo se clasifican y cómo se deben denunciar, para tener una idea más certera de lo que podemos esperar de la autoridad.

Por ello, en este ejemplar hemos incluido la nueva sección "Internet S.O.S.", con información relevante que esperamos te sea de mucha utilidad.

Comité Editorial
El Efecto Internet
www.efectointernet.org

ÍNDICE

INTERNET S.O.S. 4

INTERNET ALTERNATIVO 8

INTERNET EN TU FAMILIA 10
Internet como escenario 11
El Cortejo 13
Prevención 22
¿Ya respaldaste tu información? 24

INTERNET BIBLIOGRÁFICO 26

EL ROL DE LA ESCUELA 27
Internet y los niños 28
Robotix Challenge 2010 30

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 1. 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 Vía 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 nombrescomerciales utilizados en esta guía tienen Copyright de susdistintos titulares. Prohibida la reproducción total o parcial por cualquier medio. Todos losderechos reservados.

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 de la PGJDF

Con más de 1800 millones de usuarios conectados a Internet, es sencillo comprender que muchos de ellos, los malintencionados, ven en este universo el medio ideal para tratar de cometer sus fechorías, la mayoría de las veces sin tener que salir de sus propias guaridas.

En el mundo real, has aprendido a cuidarte de asaltos y malas experiencias identificando la forma en que los delincuentes trabajan, y evitando exponerte a ser víctima, por ejemplo, al no dejar las llaves de tu carro en su interior, no portar joyas ostentosas, etcétera.

La Unidad de Investigación Cibernética (UIC) de la Procuraduría General de Justicia del Distrito Federal, mejor conocida como la Policía Cibernética, es un grupo especializado que cuenta con una gran experiencia en el combate y prevención de los diferentes esquemas en que la red puede ser utilizada para cometer delitos en contra tuya, de tu familia o de tu patrimonio.

Por ello con este ejemplar damos inicio a esta sección en colaboración con la UIC, en donde aprenderás a identificar y cuidarte de los delitos cibernéticos.

En esta edición revisaremos un panorama general de la problemática alrededor de los delitos cibernéticos. En futuras entregas iremos profundizando en aspectos relevantes para que puedas conocer a detalle qué son, cómo prevenirlos, cómo denunciarlos, etcétera.

Existe una amplia discusión jurídica sobre la definición más precisa para el concepto “delito cibernético”. La UIC nos ofrece la que se apega más a la investigación de los mismos:

Son aquellos que se cometen mediante el uso de computadoras, sistemas informáticos u otros dispositivos electrónicos de comunicación.

Dada la enorme popularidad de Internet como medio de información y comunicación, es común asociar el concepto de delito cibernético con la red. Para todo efecto práctico, es necesario resaltar que todo lo que es delito en el mundo real, lo es también en Internet. Lo importante en toda investigación es identificar el rol que la tecnología tuvo en la comisión del ilícito, tanto como determinar cuáles tecnologías fueron utilizadas, por ejemplo, computadoras, teléfonos celulares, etcétera.

Según el rol de las Tecnologías de Información y Comunicación (TIC) utilizadas para la comisión de un delito cibernético, la UIC los clasifica en dos grupos:

- Cuando las TIC son un instrumento o medio comisivo.
- Cuando las TIC son el fin u objeto del delito.

COMO UN INSTRUMENTO O MEDIO

En esta categoría se contemplan las conductas probablemente delictivas que se valen de las computadoras como medio (utilizan métodos electrónicos para llegar a un resultado ilícito), en la comisión del delito, por ejemplo las siguientes actividades:

- Exhibición, publicación, difusión, intercambio y comercialización de pornografía infantil.
- Extorsiones, fraudes electrónicos y amenazas.
- Falsificación de documentos vía computarizada.
- Negociaciones de secuestros.
- Lectura, sustracción o copiado de información confidencial.
- Aprovechamiento indebido o violación de código para ingresar a sistemas.
- Variación del destino de sumas de dinero a otras cuentas (transferencias electrónicas).

Cabe señalar que en la mayoría de los casos, los delitos cibernéticos se adecuan a tipos penales vigentes. Por ejemplo, en el caso de un fraude bancario cometido por Internet, se perseguirá con apego al tipo penal para el "fraude", en donde Internet fue sólo el medio mediante el cual el ilícito se llevó a cabo.

COMO FIN U OBJETO

En esta categoría se contemplan las conductas probablemente delictivas que van dirigidas en contra de la computadora, accesorios o programas como entidad física. Algunos ejemplos de estas actividades son:

- Manipulación en los datos e información contenida en archivos o soportes físicos informáticos ajenos.
- Acceso a los datos y utilización de los mismos por quien no está autorizado para ello.
- Utilización del equipo y/o programas de otras personas, sin autorización, con el fin de obtener beneficios en perjuicio de otro.
- Introducción de rutinas o programas para destruir datos, información o programas.
- Utilización de la computadora con fines fraudulentos, con o sin conexión a Internet.

PROBLEMÁTICA PARA LA INVESTIGACIÓN DE LOS DELITOS CIBERNÉTICOS

Muchos factores influyen para hacer compleja la investigación y esclarecimiento de los delitos cibernéticos. En entregas posteriores iremos explicando a detalle y con diferentes ejemplos cada una de ellas, ya que en opinión de la UIC, es necesario que los usuarios de Internet conozcan lo más posible la problemática que se crea por la falta de claridad o certeza en varias etapas de la investigación, por ejemplo:

PRESENTACIÓN DE LA DENUNCIA

Es muy importante fomentar que los usuarios de Internet denuncien cualquier delito del que sean objeto, pero debemos partir de saber si lo que vamos a denunciar es en realidad un delito. Por ejemplo, mucha gente piensa que el *spam* (correo electrónico no deseado) es delito, y lo denuncian constantemente en la Línea de Denuncia de la ASI, pero no está tipificado como tal en nuestra legislación actual.

PGJ
PROCURADURIA GENERAL DE JUSTICIA DEL DF

ELEMENTOS PROBATORIOS

El usuario debe saber cómo y con qué puede demostrarle a la autoridad que fue víctima de un delito por Internet. Por ejemplo, si encontramos una página con pornografía infantil, ¿cómo se lo podemos demostrar al agente del Ministerio Público si en sus instalaciones no cuentan con acceso a Internet?

JURISDICCIÓN DE AUTORIDADES COMPETENTES

Debemos saber si un delito corresponde ser investigado por autoridades del fuero común, por las del fuero federal o por ambas.

JUDICIALIZACIÓN ADECUADA

La agencia del Ministerio Público debe integrar correctamente el expediente de la averiguación previa, con todos los elementos necesarios, y dando intervención a las autoridades capacitadas, servicios periciales, unidades de investigación cibernética, etcétera.

COLABORACIÓN DE TERCEROS INVOLUCRADOS

Hay ocasiones en que es absolutamente necesaria la cooperación de las empresas proveedoras de acceso a Internet, mejor conocidas como ISP (Internet Service Providers, por sus siglas en inglés). Por ejemplo, cuando se comete un delito desde una computadora ubicada en un café Internet.

COMPLEJIDAD INHERENTE A LA PROPIA TECNOLOGÍA

Internet nació como una plataforma de colaboración pensada para científicos y militares, por lo que los protocolos de comunicación que le dieron vida fueron desde un principio abiertos y altamente configurables. Mientras fue utilizada en este ámbito y sólo por personas de bien, esta apertura funcionó de maravilla, pero ya en la actualidad, usuarios malintencionados se aprovechan de estas características para acciones ilícitas como suplantación de identidad.

CUANTIFICACIÓN DE DAÑOS

¿Cómo puede un usuario definir con precisión cuánto exactamente vale su información en caso de ser robada?

En la medida en que los usuarios estemos mejor informados de estas y otras características de los delitos cibernéticos y su investigación, podremos aportar más y mejores elementos a la autoridad para lograr su esclarecimiento; por ello, en estrecha colaboración con la UIC, iremos presentando casos reales, y modus operandi de diferentes escenarios y modelos delictivos, tanto para estar prevenidos y no caer en ellos, como para cooperar con la autoridad al momento de tener que denunciarlos.

CASOS PRÁCTICOS PARA FACILITAR LA COMPRENSIÓN

Además, existen situaciones específicas para cada clase, que también es importante tener presente.

Veamos un caso de cuando las TIC son usadas como medio comisivo: el fraude electrónico.

La teoría del delito define dos sujetos en los delitos: el sujeto activo, que es la persona física que comete el delito, y el sujeto pasivo, que es la persona física o moral sobre quien recae el daño causado por la conducta del sujeto activo. Usualmente los definimos como delincuente y víctima, respectivamente.

Una página de Internet puede estar programada para robar información a sus visitantes y utilizarla para cometerles un fraude. Esto lo puede hacer sin su conocimiento (por ejemplo, sembrando un código malicioso en la computadora del visitante), o bien, por medio de engaños para que el propio visitante entregue su información, lo que ya de por sí modifica la forma en que deberá denunciarse en su momento. Si bien está claro que los visitantes a los que se les roba información son las víctimas, es decir, los sujetos pasivos, ¿diríamos que la página es el sujeto activo?

No, porque el sujeto activo, o delincuente, es una persona física, en este caso, el responsable de la operación de dicha página.

Dicha página puede estar alojada en otra ciudad, o en otro país, al igual que el responsable. Cuando a una persona la roban en la calle, el sujeto pasivo está en contacto con el sujeto activo. La víctima puede entonces aportar información valiosa sobre el delincuente a la autoridad para facilitar la investigación; en los delitos cibernéticos esta complejidad recae sobre la UIC, la cual deberá investigar quién es el responsable de la página.

Ahora, veamos un caso de cuando las TIC son el objeto del delito.

Supongamos que un usuario tiene almacenada en su computadora toda la información sobre planes e ideas de negocio que fue ideando durante un año. Hojas de cálculo, planes de negocio, actas de reuniones, datos estadísticos, etcétera, resultado de múltiples sesiones de trabajo, están guardados en diferentes archivos en su equipo.

¿Qué sucede si esta información es robada?

Cuando nos roban el carro, por ejemplo, y acudimos al Ministerio Público a denunciarlo, lo primero que nos solicitan es una prueba de propiedad, así que tendremos que presentar la factura correspondiente para comprobar que somos los propietarios. Si lo que nos roban es por ejemplo una cadena de oro, de la cual ya no conservamos la factura, podemos presentar a dos testigos de preexistencia del bien que declaren y confirmen que en efecto poseíamos la prenda. En ambos casos, se acredita la propiedad del bien robado y se puede dar inicio a la averiguación previa y posterior investigación del ilícito.

Pero en el caso de nuestra información, ¿cómo podemos comprobar su existencia?

Y más aún, ¿cómo podemos cuantificar su valor? ¿Se considera delito aun si la persona que la robó no le da ningún uso? ¿Cómo se determina el impacto negativo hacia nuestra propiedad?

Estas y muchas otras preguntas serán respondidas en esta sección presentándote casos prácticos, surgidos de investigaciones reales que te permitirán adentrarte en la problemática de la investigación y solución de los diferentes delitos cibernéticos, para que estés mejor informado y puedas prevenir cualquier situación desagradable al utilizar las TIC.

Estos ejemplos ilustran de forma muy básica la importancia de estar bien informado para mantener la tecnología de tu lado, y que puedas aprovecharla con toda confianza para comunicarte, investigar y divertirte de manera segura.

¿CUÁLES SON LOS DELITOS MÁS COMUNES EN INTERNET?

- Ofertas falsas de empleo.
- Fraudes financieros.
- Agencias falsas de modelos.
- El fraude nigeriano en Internet.

Éstos son algunos de los modus operandi que en colaboración con la UIC estaremos presentando en los siguientes ejemplares de *El Efecto Internet.*

Si deseas mayor información o quieres hacer cualquier comentario, escríbenos a contacto@asi-mexico.org

Unidad de Investigación Cibernética:
Red (55) 52-42-64-18, 64-20 y 64-24
gic@pgjdf.gob.mx
www.pgjdf.gob.mx/pj

Internet alternativo

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

Si tú eres diferente a todos, ¿por qué navegar como los demás? Añades ingredientes a tu pizza y tonos de llamada a tu celular, así que también puedes hacer que tu navegador se adapte a ti.

Mozilla Firefox el navegador más personal

Descarga gratis la última versión en **http://www.mozilla-europe.org/es/firefox/**

Lamborghini Murcielago dream

Manchester United Theme
por PowerslaveUk el 24/3/2010

Con Firefox, el cielo es el límite. Tú puedes extender su funcionalidad eligiendo entre más de seis mil complementos, pequeños extras que puedes descargar e instalar de forma automática y sin complicaciones. Descarga videos, sube fotos, consulta el clima o simplemente escucha música, todo desde la comodidad de tu navegador.

Y recuerda que puedes darle la apariencia que más te guste! Conoce Firefox Personas, visita www.getpersonas.com y escoge entre más de 35 000 diseños para personalizar tu navegador, o bien, crea tu propio diseño y compártelo con el mundo.

Video Downloadhelper

Descarga videos con un solo click!

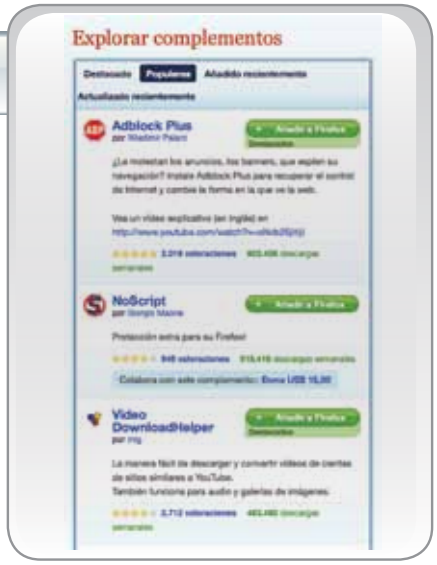
En este ejemplar, aprende cómo descargar videos de manera simple con uno de los complementos más populares de Firefox:

Video Downloadhelper.

Para visitar el directorio de complementos, sigue el enlace "Personalización" desde la página principal de descarga, o bien, visita esta liga:

https://addons.mozilla.org/es-ES/firefox

Podrás buscarlo por su nombre o descárgalo



de la lista de los más populares. Sólo tienes que hacer clic sobre el botón "Añadir a Firefox" para instalarlo automáticamente.

(Es posible que al finar te solicite reiniciar Firefox).

Video Downloadhelper

Una vez instalado, este complemento detecta si la página visitada contiene un video que pueda ser descargado, en cuyo caso el icono identificador aparece en modo animado.

Al hacer clic sobre el complemento, nos ofrece su menú de opciones:

Sólo es necesario escoger la opción "Descargar" y elegir una carpeta para almacenarlo en nuestro equipo. El complemento ofrece otras opciones interesantes como "Descargar y convertir" en caso de que el formato original no sea de nuestro agrado.

Para mayor información, se puede visitar la página del fabricante en www.downloadhelper.net

DISFRUTA 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 encontrarás información útil que te permitirá acercarte a las actividades en línea de tus hijos.

Esta publicación está dirigida principalmente a los padres de familia que necesitan saber lo que pasa en Internet, pero no tienen el tiempo o el interés de conectarse a la red.

¿POR QUÉ NECESITAN SABERLO?

Para poder orientar a sus hijos sin necesidad de convertirse en expertos de la tecnología. La buena noticia para todos los padres de familia es que lo que nos debe preocupar hoy en día no son los medios digitales que nuestros hijos utilizan, como computadoras, celulares, ipods y videoconsolas, sino las actividades que con éstos realizan y que mayormente tienen que ver con el nuevo paradigma de socialización digital. Es decir, debe preocuparnos con quién hablan, de qué hablan, qué relaciones construyen, en qué comunidades participan...

Cuando hablamos de los riesgos para menores de edad navegando por Internet, los clasificamos de la siguiente forma:

Contenido inapropiado:

A todos nos preocupa el contenido pornográfico, violento, obsceno, de drogas y demás con que nuestros hijos pueden encontrarse en línea.

Contacto inapropiado:

Los grandes beneficios de Internet no están disponibles únicamente para usuarios bien intencionados. Acosadores, depredadores y estafadores son un peligro para los menores de edad.

Conducta inapropiada:

El teórico anonimato con que navegamos en Internet puede dar lugar a conductas hostiles por parte de nuestros hijos.

En el ejemplar anterior publicamos extensivas recomendaciones sobre la forma en que puedes comunicarte con tus hijos para hablarles sobre los riesgos y de cómo prevenirlos.

En esta ocasión vamos a explorar un poco más sobre cómo las actividades de los menores de edad pueden exponerlos a riesgos que abarcan en forma mixta e incluso las tres clasificaciones. Por ejemplo, un estudiante de secundaria puede entrar a la red a buscar información sobre

“antropología” y toparse con páginas que inviten a visitar los diversos bares de la ciudad, coloquialmente conocidos como “antros”. En algunas de estas páginas pueden ofrecerse servicios de “chat”, con lo cual el menor puede iniciar una conversación con un extraño, que después de un tiempo logre invitarlo a realizar actividades inapropiadas.

La encuesta básica que la Alianza por la Seguridad en Internet (ASI) aplicó en mayo de este año entre casi 5000 alumnos del programa CENETIC Escolar, cuyas edades fluctúan entre los once y los quince años, nos reveló que:

▶23.9% se han encontrado en el mundo real con personas que conocieron en Internet.

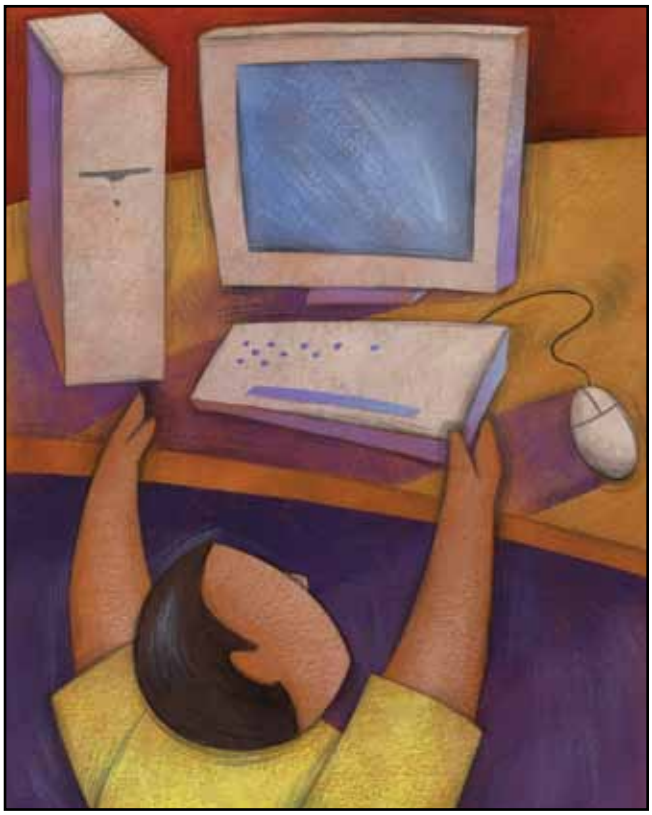
▶10.5% se han enamorado de personas a quien conocen única y exclusivamente por Internet.

▶10.4% hablan de sexo por Internet, ya sea ocasional o frecuentemente.

Nota: los resultados completos de la encuesta se pueden consultar en el repositorio de contenidos de la Alianza por la Seguridad en Internet, en www.asi-mexico.org/contenidos

Desde la puesta en marcha de nuestro portal de línea de denuncia, en www.asi-mexico.org, hemos recibido una gran cantidad de reportes sobre intentos de fraude y conductas ilegales en contra de usuarios de Internet, y los menores de edad no son la excepción, pues por medio de la tecnología suelen ser engañados para entregar información personal, participar en actividades inapropiadas y, en los casos más extremos, son contactados por usuarios malintencionados que buscan sustraerlos de sus familias con fines de trata de menores y explotación sexual y comercial infantil.

Aunado a las experiencias de nuestra línea de denuncia, nuestra organización participa en foros internacionales que estudian en forma cercana las áreas de riesgo en Internet para los menores de edad, y contamos con información valiosa sobre los esquemas de contacto de menores en



línea, principalmente el llamado “el cortejo” (o *grooming,* en inglés).

El objetivo de este documento es poner a disposición de padres de familia, autoridades escolares y usuarios de Internet en general, una descripción comprensible del proceso de contacto de menores de edad en la red, ello a modo de orientación social para que los principales responsables de la seguridad de niños y adolescentes puedan difundir medidas preventivas que ayuden a los menores a mantenerse alejados de riesgos.

I. INTERNET COMO ESCENARIO

Internet es una fantástica tecnología de información y comunicación cuyo potencial no se limita a servir únicamente a usuarios bien intencionados. Es necesario reconocer que algunos navegantes también aprovechan este gran poder para actividades ilícitas, como la trata de menores, el lenocinio de menores, el turismo sexual y la pedofilia.

Una importante recomendación inicial para todos los padres de familia es que hablen con los niños sobre este hecho en forma clara. Ellos deben saber que existen adultos que pueden tener malas intenciones en su contra para que los puedan en su momento reconocer y apartarse de ellos. Ocultárselo, o evitar tocar el tema, puede originar que el menor inadvertidamente caiga en un engaño.

En el caso de Internet, el "tronco común" en todos estos casos consiste en que la mayoría de los acosadores que buscan acercarse a un menor de edad lo hacen siguiendo un proceso sistemático llamado "el cortejo", que se describe a detalle en la siguiente sección.

Sin embargo, por su gran poder de comunicación, almacenamiento masivo de información y nuevas plataformas como las redes sociales, Internet ofrece ciertas características únicas que pueden ser explotadas por delincuentes dedicados a la trata de personas:

- Facilita el almacenamiento y disponibilidad masiva de imágenes de explotación sexual infantil para uso personal o para fines comerciales, lo que permite un tráfico intensivo entre oferta y demanda de estos contenidos.

- Las redes sociales y foros ofrecen mecanismos que pueden usarse en forma anónima para brindar el material, incluso creando comunidades que fomenten el interés por el consumo del mismo, facilitando y agilizando el contacto comercial entre compradores y vendedores, quienes aprovechan las tecnologías de cobranza y pago disponibles para cualquier negocio legítimo de comercio electrónico.

- Las llamadas "Redes punto a punto" (P2P) permiten el intercambio no supervisado de archivos de contenido ilegal.

- El volumen operacional diario de Internet hace muy difícil para cualquier autoridad la persecución de este tipo de contenido, sobre todo si se considera que, en 2010, Internet tiene aproximadamente:

a) 1800 millones de usuarios.
b) 18 000 millones de páginas web.
c) 250 millones de sitios web.

II. EL CORTEJO

Se conoce como “el cortejo”, o *grooming* (por su nombre en inglés), al proceso sistemático de acercamiento entre un acosador o depredador en línea hacia un menor de edad; el perseguidor prepara el encuentro físico entre ambos y tiene por objeto eliminar la resistencia del menor hacia los extraños y hacia contenidos inapropiados para él.

EL PROCESO DE “EL CORTEJO” CONSISTE EN SIETE ETAPAS:

1. Encuentro
Sitios populares entre los menores de edad en donde son ubicados por el acosador.

2. Compartir intereses
Desarrollan la nueva “amistad” haciendo ver al menor cuántas cosas tienen en común.

3. Ganar confianza
Se gana su confianza con un apoyo constante a sus ideas.

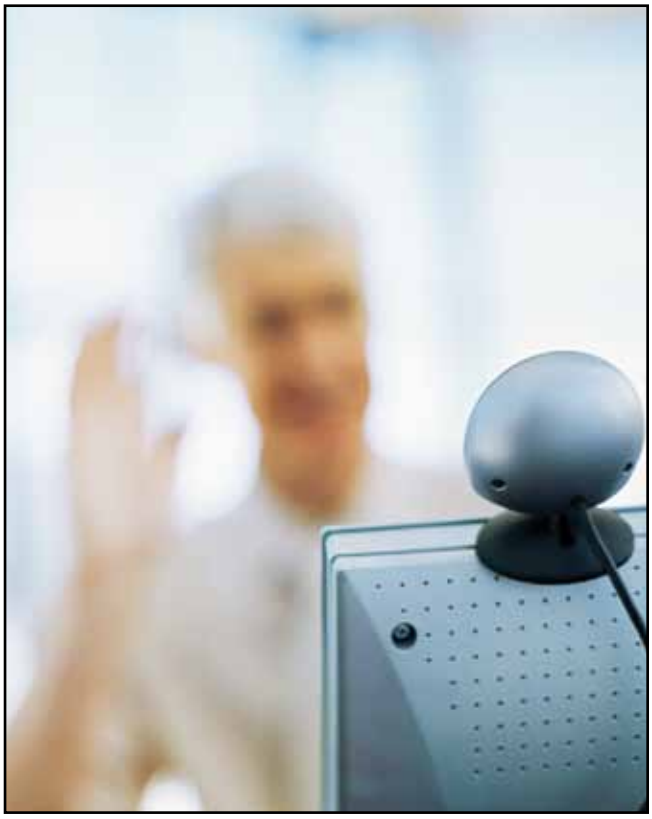
4. Obtener secretos
Desarrolla intimidad con el menor, lo convence de que son los mejores amigos, nada debe interponerse.

5. Romper barreras de resistencia
Como esta relación es diferente a todas las demás, se establecen nuevos parámetros y fronteras.

6. Amenazas
Lo adentra en la posibilidad de exponer todo lo que han hablado como amigos, se supone que son cosas privadas, o peor aún, lastimar a su familia.

7. Encuentro físico
Sin importar cómo llegó aquí, el menor siempre es la víctima.

Máximo cuidado si le pide llevar el equipo que usó en sus conversaciones, pues puede deberse a que el acosador pretende deshacerse de la



evidencia de los contactos sostenidos, frecuentemente porque sus intenciones sí son criminales.

Vale la pena mencionar que este proceso puede llevarse en promedio hasta seis meses, lo que nos deja ver que si bien no existe un estereotipo del acosador en Internet, algo que siempre los caracteriza es que son pacientes, aunque no siempre tolerantes. A continuación presentamos una descripción detallada de cada etapa.

1. ENCUENTRO

Cuando hablamos de Internet, ¿en dónde encuentra un acosador a sus víctimas menores de edad?

Los acosadores en el mundo real recurren a lugares como parques y centros comerciales para localizar a menores de edad que puedan ser de su interés para tratar de engancharlos, lo que logran mostrándoles algún juguete o dulce

que pueda llamar su atención. Diversos estudios demuestran que los pedófilos del mundo real buscan principalmente a niños menores de doce años, que pueden responder instintivamente hacia cosas materiales atractivas, como una pelota.

Pero en Internet sucede algo diferente. Las víctimas de acosadores son niños mayores de doce años que ya tienen cierta habilidad conversacional y que saben usar una computadora. A estos menores les envían mensajes y otras variantes de comunicación digital que puedan ser de su interés.

Un estudio realizado por el National Center for Missing and Exploited Children, denominado National Juvenile Online Victimization (N-JOV), cuyas conclusiones fueron publicadas en *American Psychologyst* en 2008, demuestra que el 99% de las víctimas de crímenes iniciados en Internet tenían entre trece y diecisiete años de edad, y ninguno era menor de doce años.

La legislación estadounidense contempla el concepto de "Statutory rape", que se aplica en casos en que la relación sexual entre un adulto y un menor no involucró el sometimiento por el uso de la fuerza física o moral. En México, este concepto se define en el Código Penal Federal como "Estupro":

Artículo 262. Al que tenga cópula con persona mayor de doce años y menor de dieciocho, obteniendo su consentimiento por medio de engaño, se le aplicará de tres meses a cuatro años de prisión.

Es muy importante aclarar que el Código Penal contempla otras definiciones para el delito de Violación, y algunos actos se equiparan a ésta cuando se cometen en contra de menores de edad:

Artículo 266. Se equipara a la violación y se sancionará con la misma pena:

I.- Al que sin violencia realice cópula con persona menor de doce años de edad;

EL PROCESO DE "EL CORTEJO"

ENCUENTRO 1

Sitios populares entre los menores de edad en donde son ubicados por el acosador.

COMPARTIR INTERESES 2

Desarrollan la nueva "amistad" haciendo ver al menor cuántas cosas tienen en común.

GANAR CONFIANZA 3

Se gana su confianza con un apoyo constante a sus ideas.

OBTENER SECRETOS

Desarrolla intimidad con el menor, lo convence de que son los mejores amigos, nada debe interponerse.

CONSISTE EN SIETE ETAPAS

ENCUENTRO FÍSICO

Sin importar cómo llegó aquí, el menor siempre es la víctima.

AMENAZAS

Lo adentra en la posibilidad de exponer todo lo que han hablado como amigos, se supone que son cosas privadas, o peor aún, lastimar a su familia.

ROMPER BARRERAS DE RESISTENCIA

Como esta relación es diferente a todas las demás, se establecen nuevos parámetros y fronteras.

II.- Al que sin violencia realice cópula con persona que no tenga la capacidad de comprender el significado del hecho o por cualquier causa no pueda resistirlo;

Por todo lo anterior, es lógico pensar que un acosador visite los sitios y utilice las aplicaciones que son populares entre los menores de edad, de las cuales resaltan:

- Redes sociales
- Foros (chats)
- Mensajería instantánea
- Blogs (bitácoras o diarios digitales)

Redes sociales

La especialista en socialización digital Danah M. Boyd nos da la siguiente definición:

"Una red social es un servicio en Internet que le permite a un individuo:

"a) Construir un perfil público o semippúblico dentro de un sistema bien delimitado.

"b) Articular una lista de otros usuarios con los que mantenemos algún tipo de conexión.

"c) Ver y cruzar las listas de contactos de esos usuarios con la propia para encontrar coincidencias".

Si bien hoy en día la mayoría de las redes sociales ofrecen parámetros de privacidad a sus usuarios, es un hecho que los menores de edad son especialmente descuidados con estos aspectos cuando publican información sobre ellos mismos o sus familias en las redes sociales, siendo las más populares en México Facebook, Hi5, MySpace y Twitter.

Estos parámetros de privacidad le permiten al dueño del perfil determinar qué otros usuarios pueden ver su información.

Cuando los perfiles son públicos, cualquier acosador puede tener acceso a datos que le permiten seleccionar con facilidad a posibles víctimas, como son:

- Su fotografía.
- Descripciones de sus gustos, preferencias deportivas, musicales, sociales, literarias, etcétera.
- Descripciones de sus propias personas y sus familias, que podrían facilitar su ubicación en el mundo real, como es el nombre de su escuela y la colonia donde viven.
- Narraciones de viajes recientes.
- Números de teléfono.
- Direcciones de correo electrónico.
- Lista de contactos, etcétera.

No es difícil imaginar que esta información constituye un auténtico catálogo navideño para un individuo malintencionado, por ello los padres de familia deben seguir las recomendaciones que se ofrecen más adelante, en la sección Prevención, para orientar a sus hijos sobre la privacidad en Internet.

Foros (chats)

Son servicios en Internet en que los visitantes eligen un apodo o “nickname” para participar en salas virtuales de conversación sobre afinidades y temas de interés mutuo con otros visitantes.

Existe gran cantidad de foros sobre diferentes temas, desde futbol, automovilismo, toros, viajes e intercambios, hasta negocios, astronomía, finanzas, etcétera, pero incluyendo por supuesto salas de conversación sobre sexo, drogas, alcohol, bulimia, anorexia y otros temas que podrían considerarse inapropiados para menores de edad.

Un problema existente en estos sitios es que no cuentan con elementos para validar si el visitante es mayor de edad o no; cuando mucho muestran advertencias cuando la temática del foro no es apropiada para un niño.

Mensajería instantánea

Son aplicaciones que se instalan en la computadora o dispositivo móvil del usuario y que utilizan la plataforma de Internet para permitir la comunicación directa con otros usuarios que pertenezcan a su lista de contactos.

En estricta teoría, estos servicios son más seguros, pues ningún usuario puede entrar en contacto con nosotros sin que otorguemos la autorización previa. Pero la realidad es que una gran mayoría de menores de edad acepta contactos de otras personas al menos para “averiguar” de quién se trata, y después descuidan la importancia de borrarlo de su lista si descubren que no es quien pensaban.

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

Blogs (bitácoras o diarios digitales)

Son servicios en Internet en que cualquier persona puede abrir una cuenta y crear artículos sobre temas diversos, ya sea con fines informativos o con la intención de promover debates y discusiones sobre ideas de todo tipo.

Muchos menores de edad han encontrado en los blogs un medio de expresión ideal, pues les permite desarrollar sus ideas libremente, con frecuencia sin censura alguna, y recibir retroalimentación de cualquier usuario que visite la página en donde el blog se encuentre publicado, lo que abre las puertas a que individuos malintencionados se acerquen al menor con comentarios engañosos para llamar su atención, como pueden ser felicitaciones y recomendaciones.

2. COMPARTIR INTERESES

Una vez que el acosador ha escogido a su víctima, pasa a esta etapa en la que tiene un primer acercamiento con el niño tocando temas que sabe que son de su interés, pues los encontró publicados en su perfil de red social, fue mencionado en un foro, etcétera.

Por ejemplo, si el menor ha publicado que es fanático del tenis, el acosador le enviará un mensaje con un asunto relativo a ese deporte:

"Videos de la final de Winbledon", "Mejora tus servicio en el tenis"...

El objeto de esta etapa es lograr que el menor de edad confunda al acosador con alguien que comparte sus mismos gustos. Eventualmente tocarán otros temas que igualmente son del interés del infante buscando crear una atmósfera de auténtica camaradería al plantear mensajes como "¿Te has dado cuenta de que somos tan parecidos?", hasta llegar a mensajes como " Parece ser que estamos hechos el uno para el otro!".

En esta etapa nunca se recurre a la violencia ni a la intimidación, pero si es exitoso, el acosador habrá logrado que lo identifiquen como alguien

"interesante" o "divertido", y en términos del menor de edad, "caerle bien".

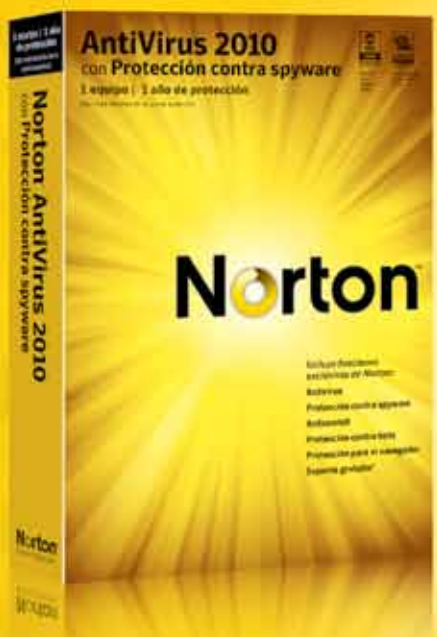
3. GANAR CONFIANZA

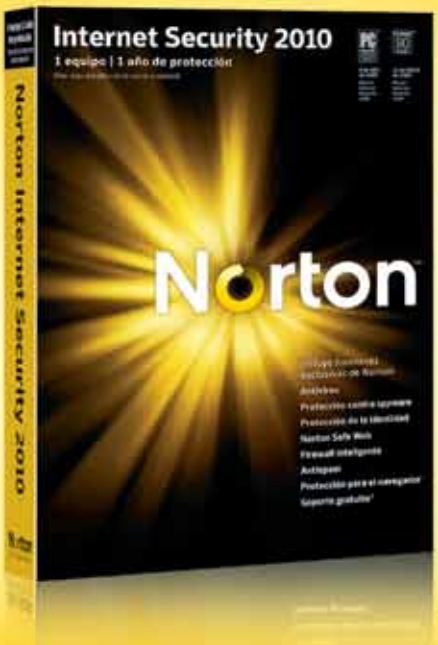
Una vez que se han establecido los lazos de intereses en común, esta etapa busca robustecer la nueva "amistad" ganándose la confianza del menor, lo que consiguen apoyando sus ideas y reforzando constantemente su autoestima.

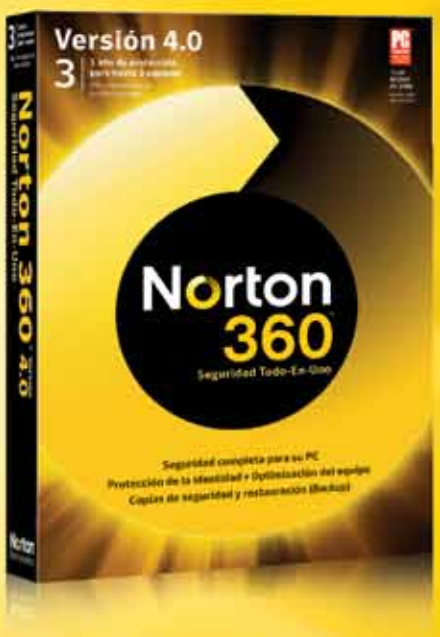
Por ejemplo, si en un blog el menor ha publicado que está en contra del trabajo forzado para otros niños en el mundo, el acosador lo felicita y le ofrece su ayuda para cosas complejas como "formar una asociación juvenil" que luche contra esa injusticia.

El objeto de esta etapa es lograr que el infante se sienta valioso y vaya asimilando que esa sen-

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

sación de bienestar la recibe mayormente cuando está en contacto con su nuevo “amigo”.

Debemos resaltar que reiteradamente el acosador le hace ver que “confía mucho en él”, y le maneja ideas como, por ejemplo, que si el mundo estuviese lleno de personas como el menor, el destino de la humanidad sería más venturoso.

Uno de los temas más explotados por los acosadores para lograr la confianza del menor es el antagonismo con sus padres, cuestión por demás recurrente entre los adolescentes. Le habla mal de los padres, le dice que “coincide” con él, que casi siempre son un estorbo, etcétera.

Si tiene éxito en esta etapa, el acosador habrá logrado que el menor lo vea como “un amigo en quien se puede confiar”, que siempre está dispuesto a escucharlo y con quien siempre se siente a gusto.

4. OBTENER SECRETOS

Ésta es una etapa muy delicada, pues toda la información secreta que el acosador logra obtener del menor puede ser usada en su contra para forzar el encuentro físico posteriormente.

Los secretos son obtenidos en forma por demás sutil, el acosador nunca recurre a pedirle abiertamente al menor que le cuente un secreto, pero recurren precisamente al escenario opuesto. Ellos mismos le preguntan al menor si “de amigo a amigo” le pueden contar “algo que lo tiene muy preocupado”, pero que es secreto y le pide que no lo comparta con nadie.

Cuando el menor acepta escucharlo, su nuevo “gran amigo” le cuenta alguna historia de su colección sobre “problemas en la escuela”, que rompió la ventana de la casa de los vecinos y sabe cómo ocultarlo, o algo más complicado, como que “robó algún artículo del centro comercial” y la policía lo descubrió...

Así logra que el menor de edad le dé consejos sobre cómo actuar, lo que agradece sobremanera, para en comunicación posterior hacerle ver que sus consejos lo ayudaron a resolver su gran problema, y manejarle que estará eternamente agradecido con su amistad y apoyo. Esto, como podemos imaginar, robustece aún más la autoestima del menor y afianza sus lazos afectivos hacia su “amigo”.

A continuación le ofrece al menor el valor de la reciprocidad, y se pone a su disposición para ayudarle con cualquier problema o necesidad de apoyo que él tenga. Es en este estado de amplia confianza en que el menor eventualmente habla de sus secretos, que pueden ser tan sencillos como haber copiado en un examen escolar, haber sacado el carro sin permiso de sus padres, o bien, haber tenido relaciones sexuales igualmente sin el conocimiento de ellos. Pueden ser cosas pequeñas o enormes, pero son siempre temas que les preocupan, y por eso han mantenido ocultos.

5. ROMPER BARRERAS DE RESISTENCIA

Durante todo el desarrollo de esta “relación”, el acosador siempre ha manejado que se trata de una amistad “única”, incomparable y diferente a cualquier otra, basada en valores como confianza, apoyo y reciprocidad. Es con base en estos supuestos que ha logrado construir una relación sólida.

Ahora, el acosador inicia una secuencia de pasos ya directamente encaminados a lograr el encuentro físico con el menor.

Lo primero que hace es tratar de “probar” la resistencia del infante ante contenidos que tengan relación con el propósito del encuentro físico, y mide su reacción, aceptación o rechazo para actuar en consecuencia.

Por ejemplo, si el objeto del encuentro será de tipo sexual, le acerca imágenes de sexo entre un adulto y un menor y analiza cómo responde el menor ante esto. Si se asusta o rechaza las imágenes, lo tranquiliza, le habla de cómo hasta en la Biblia hay gráficos de querubines que aparecen desnudos en compañía de adultos, o bien, de cómo en la literatura griega se seguían estos modelos, hasta lograr convencerlo de que este tipo de relaciones son “normales” en todos los hogares, y que si en el suyo no se presentan, es más bien porque sus padres no lo quieren.

El objeto de esta etapa es que estas imágenes sean de uso común en todas las comunicaciones entre ambos, hasta llegar al punto en que para el menor sea normal verlas y ya no le molesten.

6. AMENAZAS

Esta etapa no siempre es necesaria, pero el acosador recurre a ella cuando el menor se rehúsa a encontrarse con él en el mundo real.

Es importante señalar que las amenazas rara vez son violentas, ya que eso asustaría aún más al niño. Por el contrario, son de alguna manera hasta sutiles. Lo que hace el acosador es comentarle al menor que se encuentra “muy triste” por su negativa a conocerse en persona y que, además, no lo puede entender, ya que durante mucho tiempo han sido los “mejores amigos”, razón por la cual le sugirió conocerse para continuar fortaleciendo su amistad.

En este momento le insiste en que él no quiere causarle ningún daño, por el contrario; y le hace ver que si él fuera una mala persona y quisiera causarle algún daño, desde cuando ya hubiera revelado que el menor copió en el examen escolar, que sacó el carro sin permiso, que ya tuvo relaciones sexuales o cualquier otra información que hubiese obtenido en la etapa de secretos.

Ante la expectativa de que esa delicada información pudiera revelarse y llegar a ser del conocimiento de sus padres, normalmente el menor accede al encuentro, doblegando su resistencia.

7. ENCUENTRO FÍSICO

Las consecuencias de llegar hasta el encuentro físico con el acosador no requieren de mayor explicación, pues como podemos imaginarnos, todo tipo de ilícitos pueden cometerse en esta etapa.

Sin embargo, vale la pena mencionar que el estudio N-JOV al que nos referimos en la etapa de “Encuentro”, descubrió que el 73% de los menores que tuvieron relaciones sexuales en el primer cruce físico, repitieron estos encuentros.

Esto habla de cómo la relación que se construye durante el proceso de “el cortejo” no es agresiva para el menor y puede llegar a provocar el enamoramiento de éste con el adulto. El mismo estudio encontró que en la gran mayoría de los casos, los menores no denunciaron el encuentro porque:

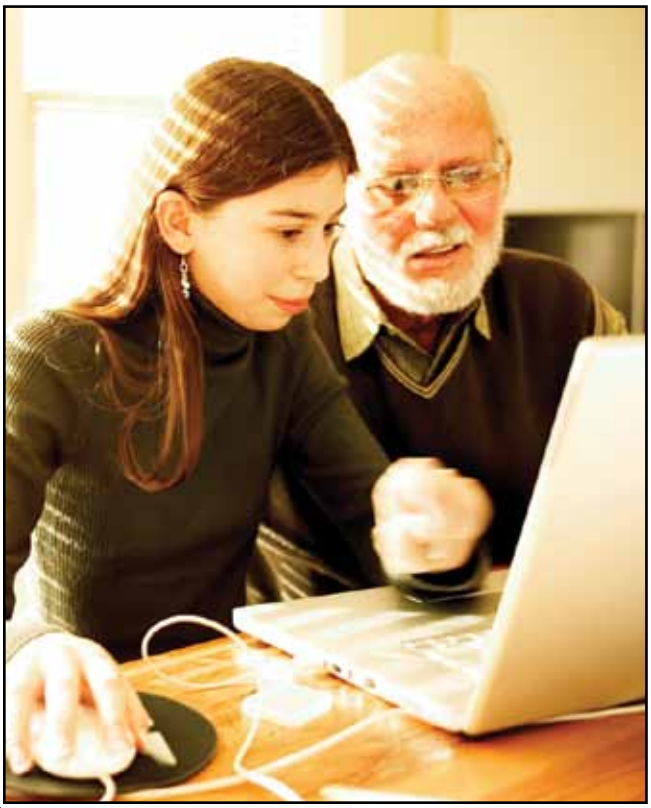
a) No sabían que era ilegal una relación entre un adulto y un menor, al menos cuando era voluntaria, y

b) No estaban sufriendo un acoso o victimización en contra de su voluntad, por el contrario, estaban incluso disfrutando la relación.

Debemos destacar que el estudio N-JOV encontró que la edad no fue un tema que al menor le interesara o que fuera un impedimento para iniciar una relación con un desconocido, ya que sólo en un 5% de los casos estudiados, el acosador tuvo que fingir ser menor de edad para ser aceptado.

Otro hallazgo interesante es que rara vez el acosador tuvo que ocultar su interés por el sexo, ya que este tema es naturalmente atractivo para cualquier adolescente.

Finalmente, una característica siempre explotada por un acosador es la ingenuidad del menor, la facilidad con que se cree historias, razón que destaca la importancia de la abierta comunicación entre padres e hijos sobre cualquier tema que estos últimos desarrollen en esta etapa.



Si necesitas más información, visita nuestro sitio en www.efectointernet.org

III. PREVENCIÓN

Toma nota de estas sencillas recomendaciones que permitirán a tus hijos utilizar las tecnologías de información y comunicación en forma segura, sana y responsable, manteniéndose alejados de posibles acosadores.

En el hogar:

Recordemos que en una relación delictiva con un acosador, el menor siempre es la víctima, por lo que se le debe dar todo el apoyo y confianza para que reporte a sus padres cualquier mala experiencia.

Ampliar la comunicación preventiva con los menores:

Es necesario informarles sin tapujos que en Internet hay adultos malintencionados que pueden buscar relaciones ilícitas con menores de edad y explicarles claramente el proceso de “el cortejo” para que lo puedan detectar y reportarlo a sus padres.

Involucrarse positivamente con la información que publican:

Es necesario conocer la información que el menor coloca en redes sociales y blogs para orientarlo sobre temas que puedan exponer su privacidad y comprometer su integridad.

Conocer sus relaciones:

Muy importante es saber con quién hablan y de qué temas platican con las personas que se relacionan en Internet.

Manifestarles confianza en el uso de tecnologías:

Los padres deben darle la confianza al menor para que les reporte malas experiencias, sin que esto le traiga como consecuencia que le castiguen la computadora o el acceso a Internet.

Desarrollar el criterio de los menores:

Los padres de familia deben enseñar pensamiento crítico a sus hijos para que sepan tomar decisiones acertadas cuando lleguen a tener contacto con personas malintencionadas en Internet.

Conocer las contraseñas de los menores:

Es muy importante hacerles saber que sus padres no desean entrometerse en sus comunicaciones personales, pero que es de suma importancia poder tener acceso a sus cuentas en caso de que lleguen a ser sustraídos de sus hogares, ya que información valiosa para las autoridades puede estar almacenada en correos y otras comunicaciones.

Practicar la parentalidad positiva:

Implica establecer límites claros y firmes para el uso de tecnologías por parte de los menores.

Mantener abierta la comunicación:

El menor debe contar con que siempre puede hablar con sus padres sobre cualquier tema que le cause molestia.

En la escuela:

Es necesario que las escuelas incorporen a sus programas académicos dos conceptos básicos para la formación de mejores usuarios de Internet.

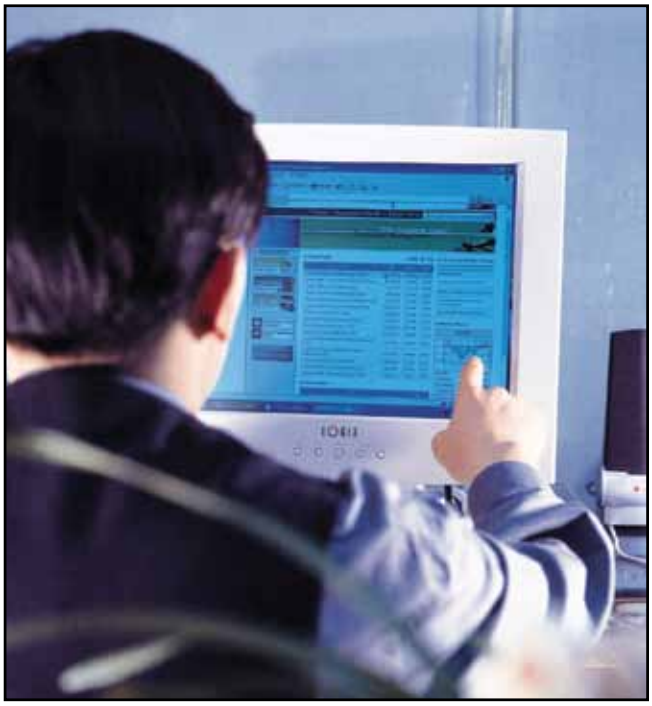
Ciberciudadanía:

Conjunto de deberes y derechos del usuario de Internet.

Temas: ciberética, reglas en el ciberespacio, mejores prácticas para la comunicación digital, libertad de expresión digital, etcétera.

Alfabetización digital:

Desarrollo de habilidades y competencias para



mejorar el criterio sobre lo que se lee y se escribe en Internet.

Temas: identidad digital, manejo de contraseñas seguras, juicio y valor digital, cultura de la privacidad...

La ASI pone a la disposición de todas las escuelas interesadas, el programa CENETIC Escolar para suministro de material educativo para la impartición de estos temas y lecciones. El programa da inicio con la aplicación de métricas en el plantel para conocer información relevante sobre el uso de Internet entre los alumnos del plantel, como son:

1. Hábitos.

2. Riesgos por contenido, conductas (hostigamiento) y por contacto con extraños (acoso).

3. Manejo de la privacidad en Internet.

Si deseas mayor información sobre este programa, por favor envía un correo a: escuelas@asi-mexico.org

¿Ya respaldaste tu información?

Las computadoras, como cualquier otro artefacto, pueden fallar en cualquier momento y uno de los problemas más comunes es que el disco duro decida "jubilarse" sin previo aviso. Lo malo es que cuando esto sucede, suele llevarse en su jubilación el montón de fotos digitales que hemos ido acumulando durante mucho tiempo, los videos de esas deliciosas vacaciones en la playa o, lo que es peor (¿será?), todos los archivos con apuntes y tareas escolares.

Ya son varias las ocasiones en las que gente conocida me busca para decirme algo como " Me urge tu apoyo! Falló el disco duro de mi computadora y perdimos toda la información. ¿Puedes ayudarnos a recuperarla?". Aunque en ocasiones lo logramos, lo cierto es que no siempre es posible y tristemente he visto casos en que se pierden miles de fotos para siempre. Para evitar esto, ¿ya respaldaste tu información?

¿Qué es un respaldo?

En pocas palabras, un respaldo no es más que una copia, total o parcial, de la información de una computadora. Esta copia se hace con el objeto de seguir teniendo la información en caso de que el original se dañe o se borre por cualquier motivo.

Sacar respaldos debería ser una tarea periódica que todo usuario de un equipo de cómputo debería realizar, pero lamentablemente hasta en grandes empresas me he encontrado con que se pierde mucha información valiosa porque los respaldos no se hacían o se hacían mal. En el caso de computadoras personales la cuestión está peor porque es frecuente que nadie nos advierta al respecto o que nos quieran ayudar con soluciones complejas y costosas. Imagínense: una vez vi a un vendedor ofertándole a un amigo un sistema de respaldo con valor de más de dos mil dólares Para su laptop de ochocientos dólares con sus tareas escolares!

¿Cómo respaldar?

Entonces, ¿qué puede hacer un usuario casero para respaldar su información de una manera barata y sencilla? Hay muchas maneras de atacar el problema, pero yo recomiendo en líneas generales algo como sigue:

a) Acostumbren a guardar su información en un conjunto de carpetas bien identificado. Por ejemplo, una carpeta para cada persona que emplea la computadora. Es aún mejor cuando debajo de dicha carpeta se tienen otras para los diversos asuntos (tareas, fotos, etcétera), pero no es necesario. Lo importante es saber dónde están todos los archivos con nuestra información y poder encontrarlos rápidamente sin tener que andar buscando por todo el disco y por cientos de carpetas en él desperdigadas.

b) Compren un disco duro externo con capacidad suficiente para almacenar sus archivos actuales y los de los próximos dieciocho meses.

c) Copien sus carpetas de datos al disco duro de manera regular, para que así puedan tener una copia de los mismos en caso de que su computadora falle.

Una nota adicional sobre el copiado: las opciones van desde realizarlo directamente con el sistema operativo de la computadora de la misma manera que copian discos entre carpetas, emplear software gratuito para sincronización de carpetas o incluso comprar un programa de respaldo individual que puede costar unos cincuenta dólares. Lo importante es siempre tener una copia para no perder nuestra información en caso de desastre.

Carpe diem.

Héctor Acevedo Juárez
hacevedoj@scitum.com.mx

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

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

SIEMPRE CONECTADOS. COMPRENDERLOS Y ORIENTARLOS.

Internet en casa: oportunidad o riesgo

Nosotros, los adultos que hemos crecido en una era sin Internet, muchas veces nos desconcertamos y no sabemos cómo reaccionar ante las nuevas tecnologías y el poder que éstas tienen sobre los niños y adolescentes. Algunas veces nos causan admiración y pensamos que son geniales y que los ayudarán a desenvolverse mejor. Pero otras, nos causan gran preocupación y hasta miedo porque llegan a ser excesivas y hasta cierto grado peligrosas.

Los padres nos encontramos navegando entre la fascinación, el desconcierto, entre las múltiples posibilidades que ofrece la red y los peligros que puede representar para nuestros niños.

Como es muy fácil acceder a Internet desde distintos lugares, es nuestra responsabilidad como padres guiar a los niños y jóvenes para que hagan un uso apropiado de la web y enseñarles a tener los ojos bien abiertos para que detecten los peligros y excesos.

Por eso, para que nuestros hijos usen las nuevas tecnologías de manera creativa, ética, crítica, y sepan cómo cuidarse dentro de este mundo virtual!, requieren nuestro apoyo y es necesario intervenir, mediar, ayudarlos y orientarlos para que realmente aprovechen en forma creativa y con fines didácticos esta nueva era virtual; en pocas palabras, lo utilicen de manera positiva.

Lograr que su uso sea limitado, bajo supervisión de un adulto según la edad, relacionándolo con otros contextos de la realidad (escuela, deportes, pasatiempos, libros, artes, etcétera), con el estímulo del adulto para pensar críticamente, conociendo los peligros de la web y elaborando normas en consenso con la familia o con los maestros de la escuela, nos permitirá estar tranquilos al ver a nuestros hijos frente a una computadora.

Computadoras, Internet, equipos devedé, cámaras digitales, mp4, libros digitales, redes sociales y seguramente muchos productos más irán apareciendo todos los días. Todo esto y mucho más es lo que hay en la web; pero tantas imágenes, tanta información, tantos juegos y tantas formas de comunicarse requieren de ciertas competencias para reorganizarse, seleccionar, canalizar y procesar todo en forma apropiada.

Por todo esto, es vital estar actualizados y conocer mejor que los niños lo que en Internet existe, lo que se puede hacer, y entender estos avances tecnológicos. Conociendo estas preocupaciones de los papás, Gabriela Alfie escribe un libro que debe ser una lectura obligada para todos los padres de familia, *Siempre conectados. Comprenderlos y orientarlos.* A lo largo de sus páginas la autora da todas las pautas, recomendaciones y medidas que se deben tomar para guiar a los niños y jóvenes en el uso adecuado de Internet.

Siempre conectados. Comprenderlos y orientarlos.
Gabriela Alfie. Alfaomega Grupo Editor, 2008.

www.alfaomega.com.mx

El rol de la escuela

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

Por su amplio impacto en el desarrollo de las sociedades, Internet ya se concibe más como una red de personas que como una red de equipos. Los usuarios debemos saber que el concepto "Seguridad en Internet", cuando se refiere a las personas, adquiere una connotación mucho más amplia, abarcando, además de la seguridad de la información misma, temas más personales como:

- Reputación
- Seguridad emocional
- Respeto a la identidad...

Al igual que cuando se habla de seguridad en el mundo real, la llamada "Seguridad en Internet" no debe entenderse como un estado, sino como un proceso de educación permanente en el que debemos estar siempre alertas a las nuevas manifestaciones de riesgos para aprender a identificarlos y apartarnos de ellos, asegurando un uso productivo y benéfico de la tecnología, siempre en nuestro favor.

Muchas escuelas, concientes de la importancia de iniciar a edad temprana esta educación, están haciendo esfuerzos importantes para lograr que sus alumnos utilicen la tecnología siempre de forma sana, segura y responsable. En esta sección estaremos presentando aportaciones ejemplares del trabajo que vienen desarrollando, para que el lector identifique el rol que cumplen en el escenario de la seguridad de los menores de edad.

En mayo pasado se aplicó en diferentes escuelas la encuesta básica sobre seguridad y privacidad en Internet, cuyos resultados iremos analizando en las siguientes entregas de esta publicación.

En esta ocasión, queremos resaltar un factor muy interesante. Mientras que casi el 76% de los alumnos consideran que colocar información personal en sus redes sociales en Internet, como nombre, teléfono y escuela, es "Peligroso" o "Muy Peligroso", más de la mitad de ellos señala que si sus perfiles se definen como "Privados", o "Sólo para sus amigos", entonces su información está a salvo.

Los reportes que recibimos en nuestra Línea de Denuncia nos dejan ver con toda claridad que casi todos los casos de difamación, humillación y hostigamiento entre menores son iniciados precisamente por un amigo, ex amigo, novio o ex novio.

Esto no hace más que resaltar la importancia de desarrollar nuevas competencias en las nacientes generaciones, que les permitan participar en el nuevo paradigma de "Socialización Digital" de forma tranquila.

El programa CENETIC Escolar le ofrece a las escuelas todo el material educativo para apoyarlas en este proceso educativo, cubriendo los temas:

- Ciberciudadanía.
- Deberes y derechos de los usuarios de Internet.
- Alfabetización digital.

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

Internet y los niños

En la actualidad existe una preocupación en nuestros maestros y padres de familia sobre los riesgos a los que están expuestos los niños y jóvenes cuando navegan en Internet.

Es un hecho que en esta época todas las personas tienen contacto con el ciberespacio, por lo que es necesario prevenir a la población más vulnerable, como son los niños y jóvenes, para evitar riesgos innecesarios.

En el Instituto Técnico y Cultural (ITYC) estamos seguros de que las mejores armas para proteger a nuestros alumnos que navegan son la orientación y la información. Utilizar esta herramienta es inevitable, por ello los criterios que el ITYC adopta cuando nuestros alumnos la utilizan son:

- Informarlos sobre el uso de Internet y sus riesgos; promover el uso adecuado en los sitios que visitan.
- Invitarlos a evitar subir su fotografía e información personal a cualquier persona sin haberlo comentado primero con sus padres.
- Recomendarles que utilicen alias en sus comunicaciones por Internet para proteger su identidad.
- Se aconseja a los menores de edad no entrar a *chatrooms* a menos que cuenten con la supervisión de un adulto. Los niños deben saber que en Internet se puede mentir fácilmente. Alguien que dice ser una niña de doce años podría ser un adulto de cuarenta con intenciones peligrosas.
- Alentarlos a informar siempre a un adulto si alguien escribe algo que no les gusta o los hace sentir incómodos.

- Pedirles que notifiquen a un adulto de su confianza si encuentran fotografías o dibujos desagradables.
- Hacerles saber que no deben creer los anuncios, las ofertas de regalos o artículos gratuitos; son trampas.
- Advertirles que no hagan citas para conocer personalmente a alguien que trataron en la red sin comentárselo primero a sus padres. En caso de realizarse la reunión, que ésta sea en un lugar público y acompañado por sus papás.

Asimismo, las recomendaciones para los padres de familia son:

- Colocar la computadora en un lugar público y abierto de la casa, donde los pequeños puedan ser supervisados.
- Que conozcan a los “amigos virtuales” de su hijo, al igual que lo hacen con los de la escuela.
- Buscar programas especializados que bloquean los sitios no apropiados para sus hijos.
- Que indiquen a su hijo que no debe llenar cuestionarios que se encuentre en Internet sin su supervisión.
- Adquirir algunas nociones informáticas que les permitan como padres conocer los peligros que existen y así saber cómo evitarlos.

Es de suma importancia comprender que Internet debe considerarse según el uso que decidamos darle. Está en nuestras manos que como padres trasmitamos a nuestros hijos la idea de convertirlo en una estupenda herramienta de estudio y consulta de información o en una peligrosa y oscura caverna llena de peligros.

En el ITYC consideramos que lo más adecuado para proteger a nuestros alumnos es ayudarlos a desarrollar criterios responsables, para que cuando se encuentren en una situación de riesgo puedan resolverla de manera segura.

Instituto Técnico y Cultural

El saber nos libera

Secundaria y Preparatoria

Primaria

Jardín de Niños

44 años

Brindando la mejor educación del país

- Excelencia académica
- Becas universitarias de excelencia
- Certificaciones en inglés, francés e informática
- Actividades extracurriculares deportivas y culturales
- Campamentos nacionales e internacionales
- Servicio de guardería y comedor vespertino

www.ityc.edu.mx

Xochicalco No. 495, Col. Narvarte México, D.F. C.P. 03600 Tels: 5543 1424 con 10 líneas.

ROBOTIX CHALLENGE® 2010

La meta de los talleres de Robótica en los colegios Peterson es ayudar a los niños a desarrollar su razonamiento lógico, su responsabilidad ante diferentes tareas, su creatividad, y demostrar que jugando pueden desplegar habilidades complejas que utilizarán a lo largo de su vida.

Los talleres de Robótica se ofrecen en los colegios Peterson, en los planteles de Cuajimalpa, Pedregal y Tlalpan. Estos talleres no sólo dan a los niños la oportunidad de desarrollar sus habilidades en la robótica e ingeniería, sino que los estudiantes también aprenden a diseñar máquinas, y este año compitieron contra los proyectos de otros alumnos de diferentes colegios del Distrito Federal durante el concurso RobotiX Challenge.

En el RobotiX Challenge 2010 participaron más de quinientos alumnos de cuarenta escuelas del área metropolitana afiliadas al programa RobotiX School. También concursaron los alumnos de tres RobotiX Centers.

La justa se realizó el 19 de junio en las instalaciones del Instituto Tecnológico de Monterrey campus Santa Fe.

Los niños participantes no despegaron los ojos del monitor de sus computadoras durante varias horas programando sus robots, afinando los últimos detalles para lograr que éstos caminaran, cargaran cajas de un lado a otro, levantaran los brazos o recorrieran distancias dentro de las maquetas de prueba.

El concurso RobotiX Challenge 2010 fue diseñado especialmente para que los niños que estudian Robótica muestren sus creaciones y habilidades y compartan con sus familiares, compañeros y con el público en general los conocimientos adquiridos.

Los elementos clave en la competencia son las computadoras, circuitos y robots programados y diseñados por los mismos niños.

El concurso constó de seis niveles y cada nivel se dividió en varias categorías de acuerdo a las edades con el fin de que todos tuvieran la misma oportunidad de ganar.

Los alumnos de los colegios Peterson mostraron sus habilidades en la competencia con excelentes resultados.

Plantel Cuajimalpa:

Primer lugar, segundo grado.

Primer lugar, tercer grado.

Plantel Pedregal:

Segundo y tercer lugares. Nivel 2. Categoría 2.

Plantel Tlalpan

Segundo lugar. Nivel 2. Categoría 6.

ROBOTIX CHALLENGE 2010

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
Secretaría de Educación Pública
ISAS Independent Schools Association of the Southwest
Association of IB World Schools

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

WiFi™ móvil en
infinitum
Navega con la conexión más rápida
en aeropuertos y en más de
149 mil sitios públicos
en todo el mundo.
parques aeropuertos universidades cafeterías restaurantes
Tiendas TELMEX
01 800 123 2222
telmex.com/infinitummovil
TELMEX®
está contigo